ORIGINAL

TRACY S. THORLEIFSON
KIAL S. YOUNG
Federal Trade Commission
915 Second Avenue, Suite 2896
Seattle, WA 98174
Tel: (206) 220-6350
Fax: (206) 220-6366

MATTHEW H. MEAD
United States Attorney
CAROL A. STATKUS
Assistant United States Attorney
2120 Capitol Avenue, 5th Floor
Cheyenne, WY 82001
Tel: (307) 772-2124
Fax: (307) 772-2123



**UNITED STATES DISTRICT COURT**
**DISTRICT OF WYOMING**

| | |
|---|---|
| **FEDERAL TRADE COMMISSION,**<br>**Plaintiff,**<br>**v.**<br><br>**ACCUSEARCH, INC. d/b/a Abika.com, and JAY PATEL,**<br>**Defendants.** | **No. 06CV0105D**<br><br>**PLAINTIFF FEDERAL TRADE COMMISSION'S DESIGNATION OF EXPERT WITNESSES** |

## 1. INTRODUCTION

Plaintiff Federal Trade Commission ("FTC") hereby designates the following expert witnesses pursuant to Fed.R.Civ.P. 26(a)(2) and U.S.D.C.L.R. 26.1(g):

1. **Cynthia Southworth, MSW**
**Director of Technology & Director of the Safety Net Project**
**National Network to End Domestic Violence**
**660 Pennsylvania Ave. SE, Suite 303**
**Washington, DC 20003**

Ms. Southworth is the leading expert on how technology intersects with domestic violence, especially how perpetrators of domestic violence use technology to locate and harm their victims. Her report, with Curriculum Vitae, publications and cases in which she has testified as an expert, is attached and incorporated by this reference. (Exhibit 1 is her report; Exhibit 1A her Curriculum Vitae; Exhibit 1B her publications; and Exhibit 1C her trainings, lectures and workshops.)

Ms. Southworth is expected to testify in accordance with the attached report that the practice of obtaining and selling consumer telephone records without the knowledge or permission of the consumer poses a grave threat to the physical and mental well-being of victims of domestic violence and stalking, sometimes resulting in physical injury or even death; that these victims cannot take reasonable steps to avoid these harms; that she is unaware of any countervailing benefits; and that the steps defendant AccuSearch, Inc., says it takes are inadequate to prevent the harm she describes. As stated in the report, her opinion is based upon her expertise and experience and her review of certain pleadings and discovery responses in this matter.

Ms. Southworth's rate is $56 per hour or $450 per day, plus reasonable travel time, costs and expenses. Particularly because of Ms. Southworth's travel schedule, if defendants were to depose Ms. Southworth, she would request that the deposition be scheduled at a date, time and place convenient to her. Plaintiffs will work with defendants to make those arrangements.

**2. Evan D. Hendricks, Editor/Publisher of *Privacy Times***
**P.O. Box 302**
**Cabin John, Maryland**

Mr. Hendricks is a long-standing, prominent expert on information privacy, including the effects that violations of privacy have on consumers. His report, with Curriculum Vitae, publications, and cases in which he has testified as an expert, is attached and incorporated by this reference. (Exhibit 2 is his report; Exhibit 2A his Background and Qualifications; Exhibit 2B his Testimony and Expert Reports; and Exhibit 2C his Curriculum Vitae.)

While Ms. Southworth focuses on severe harm to victims of domestic violence and stalking, Mr. Hendricks describes the harm to a much broader category of consumers. Mr. Hendricks is expected to testify in accordance with his report that the practice of obtaining and selling consumer telephone records without the knowledge or permission of the consumer is broadly harmful to consumers in a number of ways; that there are few if any countervailing benefits; and that the steps AccuSearch says it takes to screen customers are insufficient to prevent the harms he identifies.

Mr. Hendricks's opinions are based upon his expertise and knowledge, which is recounted in his report; his review of the same pleadings Ms. Southworth reviewed; and his review of the documents defendants had produced to plaintiffs through November 17, 2006 and the emails defendants previously produced to Congress. The documents reviewed include without limitation the invoices and emails exchanged between defendants and their third-party researchers. Some of these invoices and emails are referred to in Mr. Hendricks's report.

Mr. Hendricks respectfully wishes to reserve the right to supplement his report should additional information come to his or the FTC's attention during discovery. He charges a minimum

of $1,000 for deposition testimony ($250 per hour), which must be paid to him before the deposition begins. If the deposition exceeds four hours, the party taking his deposition needs to pay the balance at the end of the deposition. He prefers to be deposed in Bethesda, Maryland, or possibly Washington, DC, beginning no earlier than 10:00 am on a date convenient to him. If he needs to travel, his reasonable travel time and expenses must be paid in advance. Again, plaintiffs will work with defendants to make those arrangements if a deposition is requested.

Respectfully submitted this 20th day of November, 2006.

TRACY S. THORLEIFSON
KIAL S. YOUNG
Federal Trade Commission
915 Second Avenue, Suite 2896
Seattle, WA 98174
(206) 220-6350

MATTHEW H. MEAD
United States Attorney

CAROL A. STATKUS
Assistant United States Attorney
District of Wyoming
P.O. Box 668
Cheyenne, WY 82003-0668
(307) 772-2124

**CERTIFICATE OF SERVICE**

I hereby certify that on this 20th day of November, 2006, a true and correct copy of the foregoing PLAINTIFF FTC'S DESIGNATION OF EXPERT WITNESSES was served by placing same in the U.S. Mail, postage prepaid, to the following addressees:

Gay Woodhouse
Deborah L. Roden
Gay Woodhouse Law Office, P.C.
211 West 19th Street, Third Floor
Cheyenne, WY 82001

Melody Morse
Office of the United States Attorney

# Report of Cindy Southworth, MSW

I am the Founder and Director of Safety Net: the National Safe & Strategic Technology Project at the National Network to End Domestic Violence (NNEDV). While I have been working to end violence against women for over 16 years, I have focused my energies on the intersection of technology and domestic violence since 1998. I developed the Safety Net Project through trainings on technology and safety for victims in July 2000 and officially founded the project at the National Network to End Domestic Violence in August 2002. Since I am internationally recognized as the person with the greatest expertise on the intersection of technology and domestic violence, including the use of technology by stalkers, the Federal Trade Commission requested that I provide a report to address the below questions.

## A. QUALIFICATIONS

### Education and Professional Experience 1990 – 2000

As detailed in my attached resume,[1] I received a Bachelor of Science in Human Development and Family Studies from the Pennsylvania State University in State College, Pennsylvania. I earned a Master of Social Work from the University of New England in Biddeford, Maine, where I focused my coursework on ending domestic violence.

I have held positions working directly with victims of domestic violence, sexual assault, and stalking at non-profit organizations in Pennsylvania, Maine, and Washington, DC. At the Center County Women's Resource Center in Pennsylvania, I provided counseling to hundreds of victims of domestic violence and rape. My work ranged from answering countless hotline calls from victims to providing daily advocacy sessions with victims staying in the emergency abuse shelter, to assisting numerous victims through the civil protection order process at the county court house, to regularly

[1] Please see Resume, Attachment A

accompanying victims to the hospital emergency room, welfare office, and police department.

At the Abused Women's Advocacy Project in Lewiston, Maine, I worked with victims of abuse and stalking across three counties, in rural satellite offices, in the battered women's shelter, and in the program's urban protection order office. In Maine, I provided the same critical direct services as I did in Pennsylvania. In both Pennsylvania and Maine, I sat through hundreds of court hearings and trials, listening to the horrific details of injuries described by law enforcement and medical professionals. The abusers in these cases are often unexpectedly forthcoming, and appeared to feel entitled to beat, threaten, and terrorize their victims. I have found that while every victim's situation has unique elements, the lengths that an abuser went to in Pennsylvania mirrored the efforts they would use to stalk their victims in Maine.

I have also worked directly with many victims of violence through staff positions on two university campuses. At the Pennsylvania State University, I counseled students who were brutally beaten by their dating partners, assisted stalking victims in filing police reports, and was a first responder for countless sexual assaults. At the University of New England, I created a Gender Issues Program, their first campus program to address issues of violence and victim safety. Through my role at the University of New England, I worked directly with many victims of domestic violence and stalking.

I also worked to end domestic violence at the state level in both Pennsylvania and Maine. I chaired the State Legislative Committee of the Maine Coalition to End Domestic Violence, coordinated statewide efforts to address policy issues, testified in the state capitol, and responded to requests for information on domestic violence from members of the state legislature.

In Pennsylvania, I began to pair my background in technology with my work to end abuse by training law enforcement, victim advocates, and court staff about domestic violence restraining order databases on the Protection From Abuse Database Project (PFAD). I have a life-long interest and background in technology since my father has been working in the technology field since I was a toddler. I grew up with computer mother boards literally on the kitchen table and spending weekends helping repair

mainframe computers that filled an entire room. My father does technology consulting work for Interpol and private sector companies and most of my family works in some aspect of the technology field, immersing me in technology for the past thirty years. In 1998 I began to specialize in technology projects focused on ending violence against women.

During my three years with the PFAD Project, I trained judges, police, and attorneys in almost every county in the state of Pennsylvania, and at national and international conferences, on how closed justice system databases can assist in the enforcement of restraining orders. Since for safety reasons most civil and criminal domestic violence protection orders are not available online for the public, private secure databases are very important for law enforcement to be able to see a copy of the order and enforce the provisions of that order.

I have been recognized as a national domestic violence expert since 1997, when I served as a consultant to the National Domestic Violence Awareness Month Project, an initiative of the National Resource Center on Domestic Violence. As a consultant I provided guidance and research to this project on the education efforts occurring throughout all of the U.S. States and Territories. In 1998 and 1999, I served as the Outreach Coordinator and Interim Manager of VAWnet: the National Electronic Network to End Violence Against Women. VAWnet is a national Internet-based library and communications vehicle used to educate the entire country about domestic violence and sexual assault. After years of working in local shelters and training advocates and justice staff in rural and urban communities, I realized there was an unmet need in the field around training about technology's impact on victims. In 2000, I developed and presented a national training curriculum on the use of technology by stalkers, victims, and the community.

**Founder and Director of the Safety Net Project at NNEDV 2000 – Present**

After identifying the need for addressing technology misuse by stalkers and abusers, I began the Safety Net Project in 2000, providing trainings across the country while working to raise funds to move the project to the National Network to End

Domestic Violence (NNEDV). Once the project received funding in 2002, I officially founded the project and moved it to NNEDV.

The Safety Net Project educates victims of domestic and sexual violence, their advocates, and the general public on ways to use technology strategically to help escape violence and find safety. The Project also trains police officers and prosecutors on how to identify and hold perpetrators accountable for misusing technology.

The National Network to End Domestic Violence and its sister organization, the National Network to End Domestic Violence Fund, are not-for-profit organizations incorporated in the District of Columbia since 1995. NNEDV is a network of state domestic violence coalitions, representing over 2,500 shelters and hotlines across the country. NNEDV serves as the national voice of battered women and their children and those who provide direct services to them. From testifying before Congress on domestic violence issues to assisting state domestic violence coalitions in better serving the needs of the victim community, NNEDV is a national leader in efforts to assist battered women in protecting themselves and their children. The Safety Net Project works through NNEDV's national infrastructure to help victims use technology more safely and to hold offenders accountable when they misuse technology to harm their victims. As Director of the Safety Net Project, I work with practitioners, private industry, state and federal agencies, and international groups to improve safety and privacy for victims in this digital age.

**My Work as an Expert in this Unique Field**

**Publications and Trainings**

I have reviewed the entire body of published knowledge about the intersection of technology and domestic violence, and have contributed to this emerging field. In 2003, the Department of Justice's Office on Violence Against Women commissioned me and my Safety Net Project to review the literature on this new topic and write a comprehensive journal article, titled "A High Tech Twist on Abuse: Technology, Intimate Partner Stalking, and Advocacy." Following this, I was asked to write a piece for the *Family Violence Prevention and Health Practice Journal,* which was published in

December of 2005. I was also asked to write a piece titled "High Tech Violence Against Women" for the *Encyclopedia of Interpersonal Violence* (pending publication). Another piece that I co-authored is pending publication by the Sage Publications *Journal of Violence Against Women*.[2] Since the field has only recently begun to address the intersection of technology and domestic violence, the scientific studies are only beginning to emerge. In 2004, I was asked to be part of a national focus group to develop a supplement to the National Crime Victimization Survey (NCVS) to include stalking and technology. The NCVS supplement that I helped develop will begin providing national data about the use of technology in stalking in 2007 and 2008.

I travel and train local professionals every month, and often, every week, allowing me to maintain my expertise and knowledge base through regular contact with victims, victim advocates, law enforcement, privacy experts, technologists, and prosecutors throughout the country. My Safety Net Project training curriculum addresses the misuse of phone, Internet, privacy, location, and information technologies by perpetrators of domestic violence, sexual violence, and stalking. I have presented over 259 trainings based on this curriculum to over 14,885 police officers, attorneys, prosecutors, victim advocates, judges, and state agency staff.[3]

As the internationally recognized expert on technology use by stalkers, I have presented this continually updated and expanded technology and victim safety curriculum at several international trainings, including the Privacy Commission of Canada, the Department of Health Canada, the Department of Justice Canada, and the Canadian Internet Policy and Public Interest Clinic at the University of Ottawa. I have presented on technology and abuse to European-wide audiences at the Women Against Violence Europe Conferences in Copenhagen, Denmark and in Lisbon, Portugal. I have briefed representatives of the All China Women's Federation and a U.S. State Department delegation from many countries across the African continent.

---

[2] Please see list of publications, Attachment B
[3] Please see list of trainings 2000 – 2006, Attachment C

**Technical Assistance**

I serve on many national task forces and committees that address technology, privacy, and victim safety. I am a current member of the following ongoing national committees and task forces:

| Ongoing Invited Task Forces | My Role and Involvement |
|---|---|
| Department of Justice Global Information Sharing Initiative's Privacy and Information Quality Working Group | Member 2002 – Present<br>Developed, wrote, edited, and trained on multiple materials to increase victim safety and general privacy |
| Technology Committee of the National Task Force on Sexual and Domestic Violence Against Women | Chair 2003 - Present<br>Facilitated national committee to identify ways stalkers misuse technology and possible policy solutions to include in the Violence Against Women Act of 2005. |
| Anti-Spyware Coalition | Member 2005 – Present<br>Chaired panel, provided 2 keynote addresses, member of several subcommittees that develop materials on Spyware and the use of it by stalkers to monitor their victims |
| Board of Directors of the Privacy Rights Clearinghouse | Member 2005 – Present<br>Provide assistance on privacy and safety issues, help organization provide educational materials to help victims of domestic violence |

Previously I have served on the following boards, task forces, and committees:

| Prior Invited Task Forces | My Role and Involvement |
|---|---|
| Violence Against Women Online Resources (VAWOR) National Advisory Board | Member 2002 – 2005<br>Reviewed and edited multiple multidisciplinary articles for publication on the VAWOR website |
| National Public Access Portal Working Group of the U.S. Election Assistance Commission | Member June 2006<br>Provided information about risks to victims of posting voter records on the Internet and offered safer alternatives to achieve desired solution |
| National, Member of Electronic Records & Victim Safety Collaborative of the National Center on Full Faith and Credit | Member May 2005<br>Participated in an all day summit to identify safety risks to victims from electronic court records and identified an action plan to resolve some safety issues |

| | |
|---|---|
| Domestic Violence Awareness Month Project | Consultant 1997<br>Researched and Provided guidance on domestic violence awareness efforts in every state and U.S. territory |
| U.S. Department of Justice's Office on Violence Against Women | Grant Reviewer 2004<br>Reviewed and made recommendations on strengths of complex multidisciplinary grant applications to the Dept of Justice |
| Technology Privacy Focus Group sponsored by the Bureau of Justice Assistance at the U.S. Department of Justice | Member of the Steering Committee 2005<br>Designed and implemented a national multiple day symposium of technology and privacy efforts. Trained group on victim safety and stalker's technology tactics |

At the request of federal agencies, I have provided briefings to many departments including the Family Violence Prevention and Services Program at the U.S. Department of Health and Human Services, the Office on Violence Against Women at the U.S. Department of Justice, the Office of Community Services at the U.S. Department of Health and Human Services, and the Sexual Assault Prevention and Response Office of the Department of Defense.

In February 2006 I testified before a U.S. Senate Subcommittee on the dangerous impact of the sale of phone records on victims. In November 2005, I was a witness in an Administrative Hearing of the Iowa Department of Human Services to provide expert information on the ability of stalkers to track their victims through a social security number. I have also been asked to provide written comments to many agencies to address the safety of victims and stalkers misuse of technology, including:

- Comments submitted to the Centers for Disease Control around the implementation of its Health Protection Research Guide. By Cindy Southworth and Julie Field. (Jan. 2006)
- Comments submitted to Department of Defense on the proposed Sexual Assault Data Management System. By Cindy Southworth and Julie Field. (Nov. 2005)
- Comments submitted to the Federal Trade Commission on their Spyware Workshop. By Cindy Southworth and Michael C. Bisignano. (May 21, 2004)

- Comments submitted to the Superior Court of the District of Columbia on the Proposed Court Policy on Remote Public Access to Civil Case Files. By Cindy Southworth and Michael C. Bisignano. (July 2004)

- Comments on the Department of Housing and Urban Development's Homeless Management Information Systems Data and Technical Standards. By Lynn Rosenthal, Cindy Southworth and Michael Haas. (September 2002)

- Comments on the Model Policy Governing Electronic Access to Court Records. By Lynn Rosenthal, Cindy Southworth and Amy Bushyeager. (June 2002)

As the leading expert on the intersection of technology and victim safety, I have been quoted in many print materials including the New York Times, Consumer Reports, Popular Science, and have been interviewed on many radio and television outlets including CNN and the Fox News Channel.

I am frequently asked to provide insight to private and public sector groups working to balance many perspectives. For example, on the Department of Justice Global Information Sharing Initiative's Privacy and Information Quality Working Group, I balance the safety needs of victims, with the civil liberties of defendants, and with the public safety perspective of law enforcement entities. I am frequently asked by state government agencies and the federal government agencies previously listed to advise them on how to balance the technology impact on victim safety, while maintaining their mission in the public sector. In addition, I was recently asked by a large technology company to provide guidance on how to provide effective notice to consumers about a parental monitoring component of an Internet device. I was able to assist the company in finding a way to incorporate robust notice about the monitoring to victims and consumers while still creating a marketable device.

Over the past 16 years of this work, I have interviewed thousands of victims of domestic violence and stalking, and I have met hundreds of perpetrators of domestic violence in court and batterers intervention groups. From this base of experience, I have witnessed how abusers often misrepresent their motives to others, while they are startlingly forthcoming to their victims. The body of domestic violence research has identified the motives of abusers as maintaining power and control over their victims and

it is common for abusers to go to great lengths to monitor the location and activities of their victims, while in the relationship and long after the victims have fled.

I am well aware of abusers' tactics from years of work with police and other professionals who work directly with perpetrators, and also from my own interactions with batterers when they call my office, in past court hearings, and observing intervention groups. I also well aware of strategies abusers use because the abusers tell their victims, often in great detail, and the victims tell me. It is not uncommon for an abuser to tell a victim exactly how he was able to track down the victim, or keep tabs on her during the abusive relationship – in an effort to instill more fear. For example, one victim I spoke with moved across the country to escape her abuser. Once she arrived in her new town, she changed her email address and changed her cell phone number; doing this was a professional hardship since her consulting work depends on her clients being able to reach her. Within two weeks of acquiring the new phone number, her batterer called and left a threatening message. When asked how he got the victim's new number, he boasted about how easy it is to find anyone, and how little it costs. Later, he told the victim about the information broker that he had paid. He told the victim that his information broker had already spoken to her, without her realizing it was someone he had hired. Since her abuser has threatened her life on multiple occasions, his ease in finding her has caused her enormous anxiety.[4]

Within the international field of anti-violence and anti-abuse efforts, the Safety Net Project is the only national initiative specifically focused on the impact of all forms technology on victims of domestic violence. As the founder and leader of this project, and this new specialty within the field, my team has responded to over 5,000 requests for assistance in the past four years. My team responds to approximately 100 requests each month, from a broad range of individuals including, but not limited to: victims, judges, federal and state agencies, probation officers, and civil attorneys. The topics cover the entire spectrum of technology and victims, but some recent examples include: identifying the technologies and resources that were used by a perpetrator to monitor and track down his victim, helping a police officer develop the appropriate legal course of

[4] Direct communication between the victim of domestic violence and Cindy Southworth, 2006.

action to retrieve the needed evidence from phone and Internet companies through subpoenas and warrants, providing a judge with information on upcoming trainings where she could get technology stalking training, and helping a civil legal attorney and her client walk through saving an email message with the headers showing so the sender's Internet Protocol Address could be traced.

In addition to the 5,000 direct requests for assistance, over the past six years of my work with the Safety Net Project I have trained and heard from over 14,000 hotline advocates, police officers, and prosecutors who bring their cases to me so that I can provide insight into the new technologies, stalker strategies, and evidence collection.

I regularly attend and present at internationally recognized conferences, including but not limited to: Harvard's Internet Law Conference, the National Coalition Against Domestic Violence National Conference, Ending Violence Against Women International Conference, the National Association of Attorneys General Internet Victimization Conference, the International Association of Privacy Professionals Conference, the National College of District Attorneys Domestic Violence Conference, Verizon's National Domestic Violence Summit, the Women Against Violence Europe Conference, and many others.

My professional opinions below are based on 16 years working to end abuse, and my internationally recognized expertise focusing on technology, privacy, and victims. Every month I speak to a victim of domestic violence who is trying to remain hidden while her abuser hunts her down through every legitimate and unfortunately illegitimate means, including by purchasing sensitive, personal, and often illegally obtained information about that victim. Every week I talk to law enforcement officials who are trying to hold offenders accountable in a climate where every piece of personal information is for sale, for a price, whether legally or illegally obtained. Every day I talk to victim advocates who are trying to assist victims in remaining safe while perpetrators are using information brokers and other means to track them across the state or country. These victims are fleeing from brutal, and often, life threatening violence by their abusers.

## B. DESCRIPTION OF TECHNOLOGIES AND TERMS USED IN THIS REPORT

### 1) Data Miners and Information Brokers

The term "Information Broker" can apply to either an individual or company that provides information to clients, usually for a fee. The term "Data Miner," in the context of this report, refers to companies that amass and warehouse vast quantities of information about individuals. Information brokers can use biographical data collected by data miners, such as a person's maiden name or social security number, to pretext (impersonate) another individual.

### 2) Pretexting

"Pretexting" is a term that has been commonly used to describe a practice of using false pretenses to gain access to information that one typically does not have legitimate access to. An information broker might gain illegitimate access to phone records by impersonating a consumer, aided by publicly available personal consumer information or by more private information collected and sold by a data miner. Pretexting can occur when a perpetrator impersonates a victim through many communication methods, including: phone; Internet; Teletypewriter (TTY) and Relay services for the Deaf; and personal digital assistants (PDAs).

A tragic example of pretexting occurred in 1999 when Liam Youens paid Docusearch, an information broker, under $200 to obtain Amy Boyer's date of birth, social security number, and place of employment. A subcontractor of Docusearch pretexted and pretended to call to confirm Amy's insurance information and was able to illegitimately obtain Amy's employment address. After getting the information from Docusearch, Liam drove to Amy's workplace, shot and killed her, and then shot himself. Liam had been stalking Amy Boyer for several years without her knowledge. After the murder, Amy Boyer's mother sued Docusearch and the company settled out of court in 2004.[5]

[5] Ramer, Holly. "Murdered woman's mother settles suit." The Union Leader (Manchester NH) March 11, 2004 , State Edition: Pg. A1.

**3) Obtaining the Location of a Phone Owner from Phone Records**

Many online phone directories provide a reverse lookup feature. If a stalker types in a phone number, the reverse lookup features provides a victim's name, address, map, and even a satellite photo. Reverse lookup existed long before the Internet, but the directories were paper-based in the past. Now, even if a victim has an unlisted phone number, the victim's address, phone number, and a map to her house may be available to an abuser through an information broker -- since information brokers often purchase numbers from other companies that compile and provide unlisted numbers to stalkers and others.

Abusers have used victim phone records to identify businesses a victim calls (daycare, dry cleaners, bank) in order to figure out the community where she is living in hiding. For example, one stalker called many numbers listed on his victim's phone records and was able to ascertain that she was calling landlords in a small Iowa town. He eventually found and killed her.[6]

**4) Obtaining the Addresses of a Third Party from Phone Records**

In addition to using reverse lookup searches to locate the victim by the calls they make, a stalker can also use reverse lookup on the phone numbers called by a victim to find the home address and personal information of a victim's friends, family, or employer.

It is dangerous when an abuser knows the phone numbers of a victim's support system (family, friends, or an abuse shelter) since access to those phone numbers can lead the stalker to the victim and/or third parties.

**5) Obtaining the Real-Time or Recent Location of a Wireless Phone**

Since cellular and wireless phones have been on the market, it has been possible for phone carriers to obtain the geographic location of that phone using a process called triangulation. This strategy utilizes the nearby cellular or digital phone towers to pinpoint the location of a phone, by measuring the signal emitting from the cell phone to the cell towers. Triangulation should only be done by a cell phone carrier for

[6] Direct communication between Cindy Southworth and Deetive Tovar, Muscatine Police Department, 2006

legitimate purposes or at the request of law enforcement with a subpoena or warrant. However, information brokers offer to provide this information for a price, presumably illegitimately obtained.

In 2001, the U.S. Federal Communications Commission (FCC) mandated that all wireless carriers enable location tracking of their cellular/wireless phones to facilitate responses to 911 emergency calls. While a few companies chose to use triangulation, the majority of phone carriers have added Global Positioning System (GPS) chips to all new phones on their network. GPS relies on a network of satellites that orbit the earth to provide precise real-time worldwide positioning of a device. By bouncing signals off these satellites, the exact latitude and longitude of a GPS chip can be determined; providing the exact location of a victim's phone, even a street address.

Using both of these technologies, information brokers locate phones without the permission or knowledge of the phone's owner. In the past several years, a variety of information broker websites have offered to sell the location of a consumer's phone to others if they provide a phone number. The very technologies that were developed to enable police to quickly find a victim in an emergency are now being illegitimately accessed by information brokers to provide a stalker with the victim's real-time location.

**C. RESPONSE TO QUESTIONS**

I have been asked by the Federal Trade Commission (FTC) to provide my expert opinion on several questions about the impact of selling phone records on victims of domestic violence and stalking. I reviewed the following materials that I was provided by the FTC: Complaint, Briefs on Defendants' Motion to Dismiss, Defendants' Responses to Plaintiff's First Interrogatories (minus Exhibit A), Images identified by the FTC as Defendants' web site as it appeared on July 12, 2005.

My recognized leadership and expertise, combined with my education and professional experience, makes me a well qualified expert to consider these questions as they relate to victims of domestic violence and stalking.

Re: FTC v. AccuSearch, Inc., 06-CV-0105D

Dear Ms. Southworth:

As we have previously discussed, here are the questions we would like you to address in your expert report. Please call me with any questions.

1. Does the practice of obtaining and selling a consumer's personal telephone records without that consumer's permission cause harm to such consumers or to third parties? If so, please describe the types of harms that are caused or likely to be caused, the extent of such harm, and whether the consumers or third parties can take steps to avoid suffering the harm.

2. Please describe any countervailing benefits that result from the practice of obtaining and selling a consumer's personal telephone records without that consumer's permission

3 Please review the steps AccuSearch alleges it takes to ensure that it releases information only for appropriate purposes, as those steps are described in AccuSearch's Brief in Support of Defendant's Motion to Dismiss Complaint for Injunctive and Other Relief, Defendants' Responses to Plaintiff's First Interrogatories (omitting Exhibit A), and Defendants' Supplemental Responses to Plaintiff's First Set of Interrogatories. Are those steps sufficient to avoid or mitigate any harm that may come to consumers from having their telephone records sold without their permission? What steps, if any, would be sufficient?

1. Obtaining and selling a consumer's personal telephone records without that consumer's permission can cause and has caused significant harm, including death, to victims of domestic violence. Perpetrators of domestic violence and stalking pay information brokers to obtain sensitive personal information to aid them in stalking victims before, during, and after their victims leave violent relationships. Given my extensive experience in these matters, victims, victim advocates, and law enforcement regularly contact me about cases where abusers have illegitimately accessed victim information to stalk and do harm. They ask for my advice on safety strategies, evidence collection, prosecution, and more.

For example, on February 23, 2005, Luis Alberto Gomez-Rodriguez tracked his ex-girlfriend from Florida to Iowa with the aid of illegitimately obtained cell phone records and court records. Using her phone records, he tracked her from Florida, to Mississippi, Missouri, Chicago, and ultimately to Iowa. He found her new home near Iowa City and

murdered her.[7] This is a very real and deadly example of the harm that can occur when sensitive personal phone records are obtained by stalkers.

Domestic violence, sexual assault and stalking are very personal crimes; the more personal information that the perpetrator can acquire about his victim, the more dangerous and damaging the perpetrator can be. Sadly, domestic violence is quite prevalent, and women continue to be the vast majority of victims.[8] The National Institute of Justice reported that 4.9 million intimate partner rapes and physical assaults are perpetrated against U.S. women annually,[9] and millions of women are physically abused by their husbands or partners each year.[10] The effects of domestic violence are severe and devastating, and the physical injuries such as broken bones, bruises, and burns are just the start of the consequences. Victims of domestic violence also miss work due to their injuries and can ultimately lose their jobs as a result of the violence against them.[11]

Domestic Violence is about power and control, and the tactics and methods used by abusers do not change. Before abusers had access to websites offering to sell the location of their victims, they attempted to find their victims through less successful means such as calling the local abuse shelter and asking if their victim was there. While it once took a great amount of time, effort, and money to track someone, AccuSearch now provides a disturbing array of personal and sensitive information about victims, and

---

[7] Byrd, Stephen. "The hunt begins: Witnesses tell of suspect's methodical search for Muscatine couple." *The Muscatine Journal*, (Muscatine, Iowa) February 11, 2006, Available online at: http://www.muscatinejournal.com/articles/2006/02/11/news/doc43ed60933bfef871578540.txt and personal communication between Cindy Southworth and Detective Tovar, Muscatine Police Department, 2006

[8] Because the vast majority of victims of domestic violence and sexual assault are women, NNEDV will use only female nouns and pronouns throughout these comments. See Callie Marie Rennison & Sarah Welchans, U.S. Department of Justice, *Intimate Partner Violence*, at 1 (2000) (estimating that 85% of reported assaults on partners or ex-partners are committed by men against women). NNEDV acknowledges that men are also victims of domestic violence, especially in same-sex relationships.

[9] Patricia Tjaden and Nancy Thoennes, National Institute of Justice and the Centers of Disease Control and Prevention, *Extent, Nature, and Consequences of Intimate Partner Violence (2000)*; Dr. Callie Marie Rennison, Department of Justice, Bureau of Justice Statistics, *Intimate Partner Violence, 1993-2001* (February 2003).

[10] See Patricia Tjaden & Nancy Thoennes, Nat'l. Inst. of Justice, "Prevalence, Incidence and Consequences of Violence Against Women: Findings from the National Violence Against Women Survey", at 2, 7 (1998). In fact, the National Institute of Justice reported that 5.9 million assaults are perpetrated against women annually. See id. at 11. See also United States v. Morrison, 529 U.S. 598, 632 (2000) (Souter, J., dissenting) (citing estimate of four million women assault victims every year).

[11] See Susan A. Reif & Lisa J. Krisher, "Subsidized Housing and the Unique Needs of Domestic Violence Victims", *Clearinghouse* Rev. 20 (May-June 2000).

all consumers, at the abusive searcher's fingertips.

I have great concerns about many of the services offered on the AccuSearch website. Abusers and stalkers regularly use a variety of forms of phone, surveillance, and computer technologies to monitor and harass current and former intimate partners. Abusers commonly use online databases, electronic records, and paid web search engines to locate, track, and harass former partners who attempt to flee. The AccuSearch website print out that I received, dated July 12, 2005, advertises that customers can purchase unlisted numbers, details of incoming and outgoing calls from any number, drivers license information, and many other highly personal records. While I advise victims about how to protect information from public records, including sealing court records and never giving their home address to any company, this task is continuously complicated by stalkers who purchase unlisted phone numbers, cell phone records, and drivers license information. A victim can choose not to apply for a credit card in order to keep her home address confidential, but having a phone to call 911 and a drivers license to legally drive to work are essential to a victim hiding from her abuser.

In this report I provide just a few examples of the hundreds of cases I have first-hand knowledge of from my years of professional experience. Every day victims are hunted down by abusers who will use any means to locate them, harm them, and tragically, even kill them.

**Types of Harm**

**Harm to Victims of Domestic Violence and Stalking**

Harm occurs in many ways, and can have a devastating impact on the lives of victims, their loved ones, and the shelters that struggle to protect them. Victims live in dire fear of being found. Their friends and loved ones also fear and experience retaliation and violence from the batterer, and through phone records, an abuser can identify which friend, family member, or abuse shelter is currently providing safe harbor to the victim.

Unfortunately for victims of domestic violence, there are no easy escapes. Battered women often face increased violence when they attempt to flee their abusers.[12] The severity of this "separation violence" often compels women to stay in abusive relationships, rather than risk greater injury to themselves or their children. Many of those who do succeed in leaving their abuser live in constant fear of being found, which is only compounded by the potential for a victim's abuser to purchase information about the victim's location and activities.

Leaving the relationship does not stop the violence. In fact, the most dangerous time for a victim of domestic violence is when she takes steps to leave the relationship.[13] Separated women are 3 times more likely than divorced women and 25 times more likely than married women to be victims of violence at the hands of an intimate partner.[14] Many victims are stalked relentlessly for years after having escaped from their partners. These batterers who stalk their former partners, determined to hunt them down, are the most dangerous and pose the highest lethality risk.[15] Eighty percent of women who are stalked by former husbands are physically assaulted by that partner and 30 percent are sexually assaulted by that partner.[16]

Phone records are a particularly rich source of information for the determined stalker. Through illegitimately obtained phone records, a stalker can access records that include who was called, when the call was made, how long the call took, and the location of the calls. By illegitimately obtaining this information, a stalker can locate his victim without his victim even knowing that she is being tracked. For example, if the phone

---

[12] The desire to reclaim the family or retaliate can lead to sharp increases in child and spousal abuse at the time of separation. Bowker, L.H., Arbitell, M. and McFerron, J.R., "On the Relationship Between Wife Beating and Child Abuse", Yllo, K. and Bograd, M. eds., *Perspectives on Wife Abuse*, Newbury Park, CA, 1986). .

[13] Ronet Bachman and Linda Salzman, Bureau of Justice Statistics, *Violence Against Women: Estimates From the Redesigned Survey* 1 (January 2000).

[14] See Ronnet Bachman and Linda Salzman, Bureau of Justice Statistics, "Violence Against Women: Estimates From the Redesigned Survey" 1 (January 2000).

[15] Barbara J. Hart, "Assessing Whether Batterers Will Kill". (This document may be found online at: http://www.mincava.umn.edu/hart/lethali.htm), Jacqueline Campbell, "Prediction of Homicide of and by Battered Women", reprinted in *Assessing Dangerousness. Violence by Sexual Offender, Batterers, and Sexual Abusers* 96 (J. Campbell, ed., 1995).

[16] Center for Policy Research, Stalking in America, July 1997

records of a victim from Louisiana reveal to her batterer that she contacted a shelter in Utah, she is no longer safe going to that Utah shelter, though she may not realize it until it is too late.

In one recent case, a victim of domestic violence fled from the Pacific Northwest after she was severely beaten by her abuser. The batterer obtained her new cell phone records and was able to identify her location. The abuser also began to call numbers listed in her phone records, and harass these third parties, hoping to intimidate the victim into not testifying against him in the criminal case.[17]

**Financial harm**

In addition to the expenses to the victim of domestic violence, the cost to society is also substantial. The cost of intimate partner violence annually exceeds $5.8 billion, including $4.1 billion in direct health care expenses, $900 million in lost productivity, and $900 million in lifetime earnings.[18] When the costs of direct property loss, ambulance services, police response, pain and suffering and the criminal justice process are considered, the total annual cost of intimate partner violence grows to $67 billion dollars.[19]

**Real risk of homicide**

It is a tragic reality that approximately 1200 victims are murdered by their abusers each year.[20] One recent story in North Carolina highlights that abusers do track down their victims and kill them. On September 18, 2006, an abuser forced his way past

[17] Communication between Cindy Southworth and the victim's attorney, 2006.

[18] See National Center for Injury Prevention and Control, "Costs of Intimate Partner Violence Against Women in the United States", Atlanta, Ga.: Centers for Disease Control and Prevention, 2003.

[19] See Ted R. Miller et al., "Victim Costs and Consequences: A New Look", National Institute of Justice Research Report (1996).

[20] "Homicide trends in the U.S." U.S. Department of Justice · Office of Justice Programs Bureau of Justice Statistics available online at: http://www.ojp.usdoj.gov/bjs/homicide/intimates.htm

a shelter worker and shot and killed his estranged wife, Bonnie Woodring while her son was in the next room.[21]

**Harm to Third Parties**

Notably, it is not just the victims of domestic violence who are at risk if their personal information and location is revealed, but also the individuals and programs that help them. Shelters try to protect their location in the same way that individual victims of domestic violence do, by using post office boxes and unlisted phone numbers and addresses for both the shelter and for staff and volunteers. However, many shelters' emergency response teams use cell phones and pagers for on-call staff, which puts those individual staff and volunteers at risk from abusers who are trying to gain access to the shelter to find their partners. Whether the phone records obtained by an abuser or stalker are those of the shelter staff or are those of a victim who contacted the shelter, the harm can be devastating.

**Can consumers Take Steps to Avoid Suffering Harm?**

There are steps that victims can and do take to reduce their chance of being found and harmed by their stalkers. However, these steps are not sufficient to prevent harm, given the personal information provided to abusers by AccuSearch. AccuSearch, through its website Abika.com, offers search options to locate a person through cell phone records, unlisted phone records, motor vehicle records, relatives, birthdate, and even instant message name and email address. Because perpetrators use a myriad of strategies to track their victims, including services such as those offered by AccuSearch, victims often take extraordinary and desperate steps to hide their location, sometimes even changing their identities to avoid being found by their abusers. Those steps can include:

- Moving to new states;

[21] Burgess, Joel and Ponder, Brian. "Sylva woman shot to death at shelter for women"." *The Citizen Times*. (Ashville, North Carolina) September 19, 2006, Available online at: http://www.citizen-times.com/apps/pbcs.dll/article?AID=/20060919/NEWS01/60919003 and Communication between the North Carolina victim advocates and Cindy Southworth, 2006

- Using post office boxes;
- Getting unlisted phone numbers;
- Using only cell phones to avoid having utility records tied to a home phone and thus a particular address;
- Changing names through the court system;
- Changing Social Security numbers;
- Relocating to confidential shelters;
- Enrolling in state address and voter record confidentiality programs;
- Adding passwords to phone and utility accounts.
- Sealing location information in court filings; and
- Never using the Internet from a home computer.

Victims of domestic violence, acquaintance rape, and stalking are particularly vulnerable because perpetrators know so much about their victims that they can often predict where their victims may flee, and to whom they may turn for help. The phone records of the victims' loved ones are also able to be misused by an abuser if illegitimately obtained. One victim lived far from her abuser in the Southwestern part of the United States. She received relentless threatening phone calls from her ex-husband, so she continually changed her unlisted phone number. Soon after each time she changed her number, her batterer called her again. She eventually found out that her abuser was illegitimately obtaining her best friend's phone records. The victim's new number was identifiable each time, since it was the only out-of-state number called by her friend.[22]

Many of the above steps are not sufficient to protect a victim from a persistent batterer who either already knows personal information such as her passwords, or who is willing to purchase her personal information, including phone records, from unscrupulous information brokers.

[22] Communication between Cindy Southworth and the victim's advocate at a 2003 training.

2. Please describe any countervailing benefits that result from the practice of obtaining and selling a consumer's personal telephone records without that consumer's permission.

2. Since there are legitimate and legal methods for obtaining phone records, I cannot see any countervailing benefits from the practice of obtaining and selling a consumer's personal telephone records or other personal information without that consumer's permission. It is common for divorcing couples to use the subpoena process to obtain phone and financial records. It is also common for law enforcement to use subpoenas to legally obtain phone records as part of a criminal investigation. If countervailing benefits do exist, they are likely minimal because there are legal means to obtain this information.

3. Please review the steps AccuSearch alleges it takes to ensure that it releases information only for appropriate purposes, as those steps are described in AccuSearch's Brief in Support of Defendant's Motion to Dismiss Complaint for Injunctive and Other Relief, Defendants' Responses to Plaintiff's First Interrogatories (omitting Exhibit A), and Defendants' Supplemental Responses to Plaintiff's First Set of Interrogatories. Are those steps sufficient to avoid or mitigate any harm that may come to consumers from having their telephone records sold without their permission? What steps, if any, would be sufficient?

3. The steps AccuSearch alleges they take are not sufficient to mitigate any harm that may come to victims of domestic violence and other consumers. Consumers have a reasonable expectation to believe that their telephone records will not be obtained illegitimately and sold without their permission. The steps taken by AccuSearch appear to be aimed at preventing fraud and identifying searchers who request a large volume of records, such as data miners. My concern revolves around the large numbers of determined stalkers who request personal and sensitive information about their victims in order to cause harm. None of the steps that AccuSearch describes could establish whether or not the searcher is stalking a victim and intends to harm another person.

**Background Checks of Researchers and possibly Customers**

It is my experience that background checks do not reveal civil restraining and protective orders, nor do they identify many domestic violence arrests unless there is a conviction. There are many reasons for this including that a) civil and family court systems may not be connected to criminal court system, b) court records systems are often incompatible, and, c) some cases are sealed by victims to protect the privacy of their children. Additionally, since domestic violence crosses all income levels, races, ethnicity, professions, and classes, there is no way that a background check would identify most abusers or stalkers.

**Checking Email Addresses**

Many abusers and stalkers do not have a criminal record for financial crimes, so checking to see if an email address or PayPal account has been associated with fraud would not reduce the risk to a victim of domestic violence or stalking. Also an abuser can easily create new email addresses.

**Checking IP addresses**

AccuSearch's example of checking Internet Protocol (IP) addresses to ensure legitimacy of the searcher is not adequate. IP addresses can help identify where an email originated from. IP are assigned by the user's Internet Service Provider. For example, regardless of where I am in the US, if I'm using America Online (AOL), my IP address will trace back to AOL in Dulles, Virginia. Additionally, I can choose to use an anonymizer service that will route my email through any number of services, making it extremely difficult to trace the initial IP address. IP addresses cannot vouch for the character or provide information about the dangerous intention of the searcher.

**Checking PayPal**

AccuSearch further states that they check with PayPal to be sure that the searcher is verified and that payment information matches the searcher information. Similar to IP addresses, a valid PayPal account does not and cannot identify that

someone is abusive nor does it prevent a stalker from purchasing illegitimately obtained phone records.

**Suspicious Searches**

AccuSearch states that "If any type of suspicion arises for any reason, the search is not processed." It is my opinion that there is no effective screening method that would prevent abusers from stalking victims by purchasing illegitimately obtained phone records from AccuSearch. Additionally, there is nothing to prevent a stalker from lying when questioned about the reason for wanting the phone records.

How does one truly identify a suspicious search to protect a victim? Given that 1 in 4 women will experience domestic violence in her lifetime, even if AccuSearch were to cancel all requests for women's records, an abuser could still purchase the phone records of the victim's brother or father to identify her new phone number and thus location.

I believe that any request to purchase phone records is suspicious since there are legitimate and legal means, such as subpoenas and warrants.

**Canceling Searches**

AccuSearch states: "If anyone complains about a specific searcher . . ., the search will be cancelled." For a victim to complain to AccuSearch, that victim would have to know that she/he is being searched for, know that phone records were the method used by the stalker, and know that AccuSearch was the company who provided the illegitimately obtained phone records. It is my opinion that it would be difficult or impossible for victims of domestic violence or stalking to know these elements and be able to complain to AccuSearch.

**What steps to prevent harm would be sufficient?**

Stop selling phones records. AccuSearch offers the sale of sensitive and personal information about all consumers, which includes many victims of stalking and domestic violence. To prevent harm to victims, AccuSearch would need to stop selling

illegitimately obtained information, such as unlisted phone numbers, drivers license information, and phone records.

**D. CONCLUSION**

Cell phones can be a lifeline for victims of domestic violence and stalking who are trying to flee violence and build safer lives for themselves and their children. When an information broker illegitimately obtains phone and other personal records and hands them to an abuser, a victim's very life may be on the line

**EXECUTED this** 18th **day of November, 2006, at** Centreville, VA.
**[city and state]**

**Cynthia Southworth, MSW**
National Network to End Domestic Violence
660 Pennsylvania Ave. SE, Suite 303
Washington, DC 20003

Attachments:

A. Resume

B Publications

C. Trainings

Attachment A

# Cindy Southworth, MSW

**Highlights**

- Founded and direct the leading project that addresses all forms of technology use by victims of domestic violence, misuse by perpetrators, and impact of public and private sector technology on victim safety
- Worked to end domestic violence for the past 16 years at national, state, and local organizations
- Trained over 11,355 people on the intersection of technology and domestic violence since 2000
- Testified before U.S. Senate Subcommittee on the impact of the sale of phone records on victims of domestic violence
- Chair of the Technology Committee, National Task Force on Sexual and Domestic Violence
- Member of the Violence Against Women Online Resources National Board
- Member of the Department of Justice Global Information Sharing Initiative, Privacy and Information Quality Working Group

**Education**

- Masters of Social Work from the University of New England, Biddeford, ME. (1997) All coursework focused on Violence Against Women
- Bachelor of Science in Human Development & Family Studies from the Pennsylvania State University, State College, PA. (1993)

**Professional Experience**

**National Network to End Domestic Violence Fund** 2002 - present Washington, DC

***Founder and Director of Safety Net: the National Safe & Strategic Technology Project***

- Bring together and coordinate partners including Harvard Law School's Berkman Center for Internet & Society, South Asian Advocates, the PA Coalition Against Domestic Violence, and over 20 national technology and privacy experts
- Respond to over 5,000 requests for assistance from victims, their advocates, and the justice system on technology, privacy, domestic violence, and victim issues and specific stalking cases
- Supervise a team of trainers who together have trained a total 19,361 advocates and law enforcement at 367 conferences and workshops since August 2002
- Of which, personally presented trainings on the use of technology in stalking to over 14,885 advocates, police, and prosecutors at 255 conferences and workshops since July 2000.
- Author and Co-author many articles on technology and victims

**Independent Consultant** 2001 -- 2002 Harrisburg, PA

***Domestic Violence Technology Safety Consultant***

- Trained national, state, and local advocates on technology issues related to domestic violence
- Created and revised extensive technology safety and privacy curriculum for advocates
- Presented and participated in National and International Conferences


| | | |
|---|---|---|
| Cindy Southworth, MSW, Director of Technology and Director of the Safety Net Project at NNEDV | 660 Pennsylvania Ave, SE, Suite 303, Washington, DC 20003 | 202-543-5566 cs@nnedv.org |

**Pennsylvania Coalition Against Domestic Violence** 1999 – 2002 Harrisburg, PA

*Protection From Abuse Database Trainer*

- Trained court staff, law enforcement, local domestic violence advocates, and attorneys on how to most effectively use a secure online protection order database to support their work
- Presented workshops on Restraining Order Databases at regional, national, & international conferences
- Facilitated and problem solved county protection order implementation issues
- Tracked emerging court automation/privacy trends
- helped design/ test/implement protection order forms and new technology features

**National Resource Center on Domestic Violence at the Pennsylvania Coalition Against Domestic Violence** 1998 – 1999 Harrisburg, PA

*National Electronic Network on Violence Against Women Outreach & Support Coordinator & Interim VAWnet Manager*

- Managed national web-based project during transition time of roll-out to participants and while transitioning control and maintenance of $10,000 server
- Presented at national conference and to CDC/DOJ/HHS in Washington, DC in January 1999
- Organized and facilitated a bridge building meeting with sexual assault and domestic violence representatives

**Abused Women's Advocacy Project** 1997 - 1998 Auburn, ME

*Special Projects Coordinator*

- Provided counseling and advocacy for victims of domestic violence, accompanied victims to court proceeding, and answered the 24 hour hotline
- Assisted with Batterers Intervention Group
- Trained police and community members
- Initiated transitional housing program for victims with complex issues
- Trained staff, interns, and volunteers on domestic violence
- Co-wrote successful trauma safe house grant application
- Chair of statewide legislative committee for the Maine Coalition the End Domestic Violence
- Supervised and coordinated volunteer/intern/staff training, facilitated complex staff issues in working with survivors with extraordinary obstacles
- Organized all domestic violence awareness month activities

**University of New England** 1995 –1997 Biddeford, ME

***Gender Issues Intern/Graduate Assistant/Computer Technician***

- Designed and Implemented a gender issues research project leading to a Gender Issues Center
- Contributed in all arenas of administering the graduate Social Work Program and participated in all faculty committees and meetings as sole student representative
- Installed network cards in new computers, installed software and settings from the network

**Centre County Women's Resource Center** 1992 – 1995 State College, PA

***Domestic Violence Housing Case Manager, Overnight Shelter Counselor, Child Sexual Abuse Prevention Coordinator***

- Coordinated all aspects of a domestic violence transitional housing program for families, counseled victims, provided legal advocacy to victims
- Trained law enforcement and members of the community on domestic violence
- Coordinated all aspects of a child abuse prevention program to children ages 5-9, presented
- Provided domestic violence and sexual assault crisis services, legal advocacy, prevention programs, and training to volunteers/interns
- Organized state-wide meeting of all housing programs to facilitate improved services and advocacy

**Pennsylvania State University** 1990 – 1993 State College, PA

***Office of Residence Life, Resident Assistant, Instructor***

- Taught 3-credit course for counselors on domestic violence, sexual assault, and other issues
- Provided crisis counseling to students
- Presented educational sessions on abuse, health, and other topics

**Technology Background**

- Expert on technology strategies and systems used by stalkers, privacy and court records, privacy and electronic justice information systems, surveillance technology and victim safety
- Presented computer hardware & software training and provided technical support to domestic violence advocates, court staff, law enforcement, social workers, & academics
- Managed technology projects, procured equipment and software solutions, coordinated the work of technology consultants, designed and implemented project evaluation
- Versed in privacy enhancing technologies, encryption & security concepts, database privacy issues, DSL/broadband, computer crime/stalking/monitoring, and telecommunication privacy levels
- Versed in multiple word processing, graphic design, internet, database, spreadsheet applications, hardware & software installation, and beta-testing technology features

| | | |
|---|---|---|
| **Additional Experience** | Chair, Technology Committee of the National Task Force on Domestic and Sexual Violence | 2003 - 2005 |
| | Member of the Department of Justice, Office of Justice Programs' Global Justice Information Sharing Initiative's Privacy and Information Quality Working Group. | 2002 - Present |
| | Member of the Anti-SpyWare Coalition | 2005 - Present |
| | Member of the Violence Against Women Online Resources National Advisory Board | 2002 - 2005 |
| | Consultant, National Domestic Violence Awareness Month Project | 1997 |
| | Consultant, Maine Communities Face Alcohol | 1997 |


| | | |
|---|---|---|
| Cindy Southworth, MSW, Director of Technology and Director of the Safety Net Project at NNEDV | 660 Pennsylvania Ave, SE, Suite 303, Washington, DC 20003 | 202-543-5566 cs@nnedv.org |

Attachment B

# Publications of Cindy Southworth, MSW

Publications as primary author, co-author, and
co-author through the Safety Net Project which Ms Southworth directs.

**2006**

- Comments submitted to the Centers for Disease Control around the implementation of its Health Protection Research Guide. By Cindy Southworth and Julie Field. (Jan. 2006)
- *Protecting Consumers' Phone Records*. Testimony given before the Subcommittee on Consumer Affairs, Product Safety, and Insurance. United States Senate. (February 8, 2006)
- *Tech Savvy Teens. Tips For Raising Awareness on Information, Privacy, & Internet*. By the Safety Net Project. (2006)
- *Update on HMIS, VAWA 2005 & Confidentiality*. By the Safety Net Project. (2006)
- *Web Wise Women. Minimizing information published about you on the World Wide Web.* By the Safety Net Project (rev. 2006). Available in Spanish.
- *Technology, Stalking and Domestic Violence Victims.* By Cindy Southworth and Sarah Tucker, National Association of Attorneys General and National Center for Justice and the Rule of Law at the University of Mississippi School of Law. (pending publication)

**2005**

- Comments submitted to Department of Defense on the proposed Sexual Assault Data Management System. By Cindy Southworth and Julie Field. (Nov 2005)
- *A High-Tech Twist on Abuse: Technology, Intimate Partner Stalking, and Advocacy*. By C. Southworth, S. Dawson, C. Fraser, and S. Tucker. (2005)

- *A High-Tech Twist on Abuse.* By S. Tucker, T. Cremer, C. Fraser, & C. Southworth (December 2005). Article in Volume 1, Issue 3 of the online journal: *Family Violence Prevention and Health Practice*.

- *Prioritizing the Confidentiality & Safety of Victims: Questions to Consider for Multi-agency or Co-located Sites*. By the Safety Net Project. (2005).

- *The President's Family Justice Center Initiative's Confidentiality, Information Sharing, and Privacy Protocol Recommendations.* Prepared by the National Network to End Domestic Violence, the San Diego Family Justice Center Foundation, and the Office on Violence Against Women of the United States Department of Justice. (August 2005).

- *Technology Safety Planning with Survivors. Tips to discuss if someone you know is in danger.* By the Safety Net Project. (rev. 2005). Available in English, Spanish, Vietnamese, Chinese, Korean, Somali, and Russian.

- *Intimate Partner Stalking, Technology, and Stalking.* By C. Southworth, J. Finn, S. Dawson, C. Fraser, and S. Tucker. Sage Publications: *Journal of Violence Against Women*. (pending publication).

**2004**

- Comments submitted to the Federal Trade Commission on their Spyware Workshop. By Cindy Southworth and Michael C. Bisignano. (May 21, 2004)

- Comments submitted to the Superior Court of the District of Columbia on the Proposed Court Policy on Remote Public Access to Civil Case Files. By Cindy Southworth and Michael C. Bisignano. (July 2004)

- *Data Security Checklist to Increase Victim Safety & Privacy.* By the Safety Net Project. (rev. 2004). Available online.

- How Tracking Systems Place Victims at Risk. Homeless Management Information Systems & Victims of Abuse and Stalking. By the Safety Net Project. (April 2004)

- *Public & Internet Access to Court Records. Safety & privacy risks for victims of domestic violence & all citizens using the justice system.* By the Safety Net Project. (rev. 2004).

- The State of the States. Responses to victim safety and HMIS. By the Safety Net Project. (May 2004)

- *Tips for Survivors of High-Tech Abuse and Stalking.* By the Safety Net Project. (rev. 2004). Available in Spanish, Chinese, Korean, Vietnamese, Somali, & Russian.

- *Website Safety Alerts. Tips for Advocacy Organizations.* By the Safety Net Project. (rev. 2004).

**2002**

- Comments on the Department of Housing and Urban Development's Homeless Management Information Systems ("HMIS") Data and Technical Standards. By Lynn Rosenthal, Cindy Southworth and Michael Haas. (September 2002)

- Comments on the Model Policy Governing Electronic Access to Court Records. By Lynn Rosenthal, Cindy Southworth and Amy Bushyeager. (June 2002)

Attachment C

# Cindy Southworth, MSW
# Trainings, Keynotes, and Workshops

Total People Trained by Ms Southworth 2000 - 2006 14,885

Total Trainings, Keynotes, & Workshops 2000 - 2006 259

| Breakdown of Ms Southworth's trainings | |
|---|---|
| Local Workshops | 54 |
| Statewide Trainings | 88 |
| National Keynotes | 108 |
| International Trainings | 9 |
| Total | 259 |

| Safety Net Project (Team) Totals 2002-2006 | |
|---|---|
| Total requests for assistance responded to (on cases, educational materials, etc) | 5319 |
| Total Number of Trainings completed by the Safety Net Team | 367 |
| Total people trained by the Project | 19,371 |

## List of Trainings presented by Cindy Southworth, MSW 2000-2006

| | Date | Sponsor | Training Topic | Location | # | Type |
|---|---|---|---|---|---|---|
| 1. | Jul-00 | National Coalition Against Domestic Violence National Conference | Technology Use By Abusers, Victims & Their Advocates | Portland, OR | 80 | National |
| 2. | Mar-01 | Pennsylvania Coalition Against Domestic Violence Statewide Conference | Understanding Computer Technology for Domestic Violence Advocates | State College, PA | 8 | State |
| 3. | Mar-01 | Pennsylvania Coalition Against Domestic Violence Statewide Conference | Safer Technology Use for Victims | State College, PA | 13 | State |
| 4. | Mar-01 | Pennsylvania Coalition Against Domestic Violence Statewide Conference | Court Technology for Advocates | State College, PA | 9 | State |

| | Date | Sponsor | Training Topic | Location | # | Type |
|---|---|---|---|---|---|---|
| 5. | Jul-01 | Support Network for Battered Women | Technology Use By Abusers, Victims & Their Advocates | Waltham, MA | 20 | Local |
| 6. | Jul-01 | Abused Women's Advocacy Project | Technology Use By Abusers, Victims & Their Advocates | Lewiston, ME | 20 | Local |
| 7. | Sep-01 | Focus Group and Training for Advocates | Technology Use By Abusers, Victims & Their Advocates | St Paul, MN | 15 | Local |
| 8. | Feb-02 | Battered Women's Justice Project & the National Clearinghouse for the Defense of Battered Women: *Coalition Advocates & Attorney Network* National Meeting | Technology Use By Abusers, Victims & Their Advocates | Memphis, TN | 30 | National |
| 9. | May-02 | Battered Women's Justice Project National Conference | Cyberstalking: Technology Use By Abusers, Victims & Their Advocates | Spokane, WA | 90 | National |
| 10. | May-02 | The Berkman Center on Internet and Society at Harvard Law School, Guest Lecture for Berkman Online Lectures & Discussions | Violence Against Women on the Internet, Victim Safety Module | Online Course | N/A | National |
| 11. | Jun-02 | Pennsylvania Coalition Against Domestic Violence Statewide Trainings | Technology Use By Abusers, Victims & Their Advocates | Harrisburg, PA | 65 | State |
| 12. | Jun-02 | Pennsylvania Coalition Against Domestic Violence Statewide Trainings | Understanding Technology for state domestic violence coalition staff | Harrisburg, PA | 55 | State |
| 13. | Jun-02 | Battered Women's Justice Project: Working With Battered Women in the Criminal & Civil Justice Systems: Strategies for Advocates | Cyberbattering: Technology Use By Abusers, Victims & Their Advocates | Minneapolis, MN | 80 | National |
| 14. | Jun-02 | Battered Women's Justice Project: Working With Battered Women in the Criminal & Civil Justice Systems: Strategies for Advocates | Technology Use By Abusers, Victims & Their Advocates | Minneapolis, MN | 25 | National |
| 15. | Jun-02 | American Prosecutors Research Institute & The Battered Women's Justice Project | Cyberstalking and High-Technology Battering | Tucson, AZ | 55 | National |
| 16. | Jul-02 | The Berkman Center for Internet & Society at Harvard Law School: iLaw 2002 -Internet Law Program | Violence Against Women on the Internet – strategies and safety issues | Cambridge, MA | 25 | National |

| | Date | Sponsor | Training Topic | Location | # | Type |
|---|---|---|---|---|---|---|
| 17. | Aug-02 | National Coalition Against Domestic Violence National Conference | Technology Use By Abusers, Victims & Their Advocates | Orlando, FL | 40 | National |
| 18. | Aug-02 | National Network to End Domestic Violence Fund | Technology Use By Abusers, Victims & Their Advocates | Providence, RI | 10 | National |
| 19. | Sep-02 | National District Attorney's Association | Introduction to Cyberstalking | Columbia, SC | 75 | National |
| 20. | Sep-02 | National District Attorney's Association | Outside the Email Envelope: Helping victims respond to Domestic Violence Cyberbattering | Columbia, SC | 69 | National |
| 21. | Sep-02 | Tri-County Domestic Violence Coordinating Council | Technology Use By Abusers, Victims & Their Advocates | Portland, OR | 40 | Local |
| 22. | Sep-02 | State Coalition Advocates & Attorney Network | Strategies for helping victims & advocates keep victim data off public websites | Portland, OR | 68 | National |
| 23. | Sep-02 | State Coalition Advocates & Attorney Network | Technology Use By Abusers, Victims & Their Advocates | Portland, OR | 72 | National |
| 24. | Oct-02 | ASHA South Asian Domestic Violence Program | Technology Use By Abusers, Victims & Their Advocates | Washington DC | 20 | Local |
| 25. | Oct-02 | National District Attorney's Association | Introduction to Cyberstalking | Columbia, SC | 75 | National |
| 26. | Oct-02 | National District Attorney's Association | Outside the Email Envelope: Helping victims respond to Domestic Violence Cyberbattering | Columbia, SC | 65 | National |
| 27. | Oct-02 | National Network to End Domestic Violence Fund | Technology Use By Abusers, Victims & Their Advocates | St Louis, MO | 15 | National |
| 28. | Oct-02 | Tri-County Domestic Violence Coordinating Council | Technology Use By Abusers, Victims & Their Advocates | St Louis, MO | 40 | Local |
| 29. | Oct-02 | Indiana Coalition Against Domestic Violence & an Indianapolis Local Program | Data Safety for Victims of Domestic Violence & their advocates | Indianapolis, IN | 14 | Local |
| 30. | Oct-02 | Indiana Coalition Against Domestic Violence & an Indianapolis Local Program | Technology Use By Abusers, Victims & Their Advocates | Indianapolis, IN | 16 | Local |
| 31. | Nov-02 | William & Mary Law School's Courtroom 21 High Tech Courtroom Project | Protecting Victims while providing greater online access to court records | Williamsburg, VA | 100 | National |
| 32. | Nov-02 | National Network to End Domestic Violence Fund | Technology Use By Abusers, Victims & Their Advocates | Miami, FL | 65 | National |

| | Date | Sponsor | Training Topic | Location | # | Type |
|---|---|---|---|---|---|---|
| 33. | Nov-02 | Miami Dade Domestic Violence Coordinating Council & FL Coalition | Technology Use By Abusers, Victims & Their Advocates | Miami, FL | 35 | Local |
| 34. | Nov-02 | Pennsylvania Coalition Against Domestic Violence | Email Safety Issues for Victims of Domestic Violence | Harrisburg, PA | 40 | State |
| 35. | Dec-02 | California Alliance Against Domestic Violence | Technology Use By Abusers, Victims & Their Advocates | San Jose, CA | 20 | Local |
| 36. | Dec-02 | American Prosecutors Research Institute and the Battered Women's Justice Project | Technology Issues for Immigrant Victims of Domestic Violence | San Francisco, CA | 50 | National |
| 37. | Dec-02 | National Network to End Domestic Violence Fund | Technology Issues for Coalitions & Advocates | San Diego, CA | 10 | National |
| 38. | Dec-02 | California Alliance Against Domestic Violence | Technology Use By Abusers, Victims & Their Advocates | San Diego, CA | 45 | Local |
| 39. | Dec-02 | Washington State Coalition Against Domestic Violence | Technology Use By Abusers, Victims & Their Advocates | Seattle, CA | 60 | Local |
| 40. | Dec-02 | Alaska Network on Domestic Violence and Sexual Assault | Technology Use By Abusers, Victims & Their Advocates | Juneau, AK | 50 | State |
| 41. | Jan-03 | Alexandria Domestic Violence Program (DVP) | Technology Use By Abusers, Victims & Their Advocates | Alexandria, VA | 25 | Local |
| 42. | Jan-03 | Illinois Coalition Against Domestic Violence | Data Safety for Victims of Domestic Violence & their advocates | Springfield, IL | 50 | State |
| 43. | Jan-03 | National Center for Victims of Crime | Technology Use By Abusers, Victims & Their Advocates | Washington, DC | 30 | National |
| 44. | Jan-03 | Stalking Resource Center at the National Center for Victims of Crime | Cyberstalking | Washington, DC | 10 | National |
| 45. | Feb-03 | Texas Council on Family Violence | Technology Use By Abusers, Victims & Their Advocates | Austin, TX | 70 | State |
| 46. | Feb-03 | National Alliance to End Homelessness | Data Safety for Victims of Domestic Violence & their advocates | Washington, DC | 15 | National |
| 47. | Feb-03 | Texas Council on Family Violence | Technology Use By Abusers, Victims & Their Advocates | Austin, TX | 30 | State |
| 48. | Feb-03 | National Domestic Violence Hotline | Technology Use By Abusers, Victims & Their Advocates | Austin, TX | 20 | National |
| 49. | Feb-03 | National Network to End Domestic Violence National Training of Trainers | Technology Use By Abusers, Victims & Their Advocates | Dallas | 70 | National |
| 50. | Feb-03 | National Network to End Domestic Violence National Training of Trainers | Data Safety for Victims of Domestic Violence & their advocates | Dallas | 70 | National |

| | Date | Sponsor | Training Topic | Location | # | Type |
|---|---|---|---|---|---|---|
| 51. | Feb-03 | Indiana Coalition Against Domestic Violence | Technology Use By Abusers, Victims & Their Advocates | South Bend, IN | 25 | State |
| 52. | Feb-03 | Indiana Coalition Against Domestic Violence | Technology Use By Abusers, Victims & Their Advocates | Bloomington, IN | 25 | State |
| 53. | Mar-03 | Stalking Resource Center at the National Center for Victims of Crime | Technology Use By Abusers, Victims & Their Advocates | Memphis | 90 | National |
| 54. | Mar-03 | National Network to End Domestic Violence Southern State Coalition Meeting | Technology Use By Abusers, Victims & Their Advocates | Atlanta, GA | 10 | National |
| 55. | Mar-03 | Florida Coalition Against Domestic Violence Statewide Rural Conference | Technology Use By Abusers, Victims & Their Advocates | Marianna, FL | 30 | State |
| 56. | Mar-03 | Florida Coalition Against Domestic Violence Statewide Rural Conference | Technology Use By Abusers, Victims & Their Advocates | Marianna, FL | 30 | State |
| 57. | Mar-03 | Stalking Resource Center at the National Center for Victims of Crime National Conference | Data Safety for Victims of Domestic Violence & their advocates | Memphis | 35 | National |
| 58. | Mar-03 | Stalking Resource Center at the National Center for Victims of Crime National Conference | Data Safety for Victims of Domestic Violence & their advocates | Memphis | 25 | National |
| 59. | Mar-03 | Memphis Regional Task Force on Domestic Violence | Technology Use By Abusers, Victims & Their Advocates | Memphis | 25 | Local |
| 60. | Apr-03 | West Virginia State Domestic Violence Coalition Day Long Training | Technology Use By Abusers, Victims & Their Advocates | Charleston, WV | 85 | State |
| 61. | May-03 | National Network to End Domestic Violence | Technology Use By Abusers, Victims & Their Advocates | Seattle, WA | 10 | National |
| 62. | May-03 | National Coalition of Anti-Violence Programs: National Conference | Technology Use By Abusers, Victims & Their Advocates | Philadelphia, PA | 30 | National |
| 63. | May-03 | Association of Threat Assessment Professionals | Technology Use By Abusers, Victims & Their Advocates | Fairfax | 65 | Local |
| 64. | May-03 | Pennsylvania Coalition Against Domestic Violence | Technology Use By Abusers, Victims & Their Advocates | Harrisburg, PA | 15 | State |
| 65. | May-03 | Pennsylvania Coalition Against Domestic Violence | Technology Use By Abusers, Victims & Their Advocates | Harrisburg, PA | 25 | State |
| 66. | May-03 | Delaware Coalition Against Domestic Violence | Technology Use By Abusers, Victims & Their Advocates | Rehoboth | 40 | State |
| 67. | May-03 | Delaware Coalition Against Domestic Violence | Technology Use By Abusers, Victims & Their Advocates | Rehoboth | 45 | State |
| 68. | Jun-03 | Marine Corps Victim Advocacy Program Conference | Technology Use By Abusers, Victims & Their Advocates | Quantico, VA | 40 | National |

| | Date | Sponsor | Training Topic | Location | # | Type |
|---|---|---|---|---|---|---|
| 69. | Jun-03 | Battered Women's Justice Project: *After the First response: Promising Advocacy Practices* | Technology Use By Abusers, Victims & Their Advocates | Providence, RI | 120 | National |
| 70. | Jun-03 | New York State Coalition Against Domestic Violence Day Long Training | Technology Use By Abusers, Victims & Their Advocates | New York, NY | 40 | State |
| 71. | Jun-03 | Rhode Island Coalition Against Domestic Violence Day Long Training | Technology Use By Abusers, Victims & Their Advocates | Providence, RI | 50 | State |
| 72. | Jun-03 | Maryland Network Against Domestic Violence Statewide Conference on Cyberstalking | Technology Use By Abusers, Victims & Their Advocates | Baltimore, MD | 200 | State |
| 73. | Jun-03 | Florida Coalition Against Domestic Violence Legal Clearinghouse Training for Lawyers | Technology Use By Abusers, Victims & Their Advocates | Orlando, FL | 60 | State |
| 74. | Jun-03 | Battered Women's Justice Project: *After the First response: Promising Advocacy Practices* | Technology Use By Abusers, Victims & Their Advocates | Providence, RI | 30 | National |
| 75. | Jul-03 | National Conference on Homelessness | Data Safety for Victims of Domestic Violence & their advocates | Washington, DC | 70 | National |
| 76. | Jul-03 | Maryland Network Against Domestic Violence | Technology Use By Abusers, Victims & Their Advocates | Bowie, MD | 25 | State |
| 77. | Aug-03 | National Intimate Partner Stalking Conference | Technology Use By Abusers, Victims & Their Advocates | Portland, OR | 50 | National |
| 78. | Aug-03 | Pennsylvania Coalition Against Domestic Violence | Data Safety for Victims of Domestic Violence & their advocates | Harrisburg | 25 | State |
| 79. | Aug-03 | Pennsylvania Coalition Against Domestic Violence | Data Safety for Victims of Domestic Violence & their advocates | Harrisburg | 10 | State |
| 80. | Aug-03 | Stalking Resource Center at the National Center for Victims of Crime National Conference | Technology Use By Abusers, Victims & Their Advocates | Portland OR | 100 | National |
| 81. | Aug-03 | Fairfax County Domestic Violence Task Force | Technology Use By Abusers, Victims & Their Advocates | Fairfax VA | 20 | Local |
| 82. | Aug-03 | Multnomah County Domestic Violence Coordinator's Office & The Oregon Coalition Against Domestic & Sexual Violence | Technology Use By Abusers, Victims & Their Advocates | Portland OR | 50 | Local |

| | Date | Sponsor | Training Topic | Location | # | Type |
|---|---|---|---|---|---|---|
| 83. | Aug-03 | Multnomah County Domestic Violence Coordinator's Office & The Oregon Coalition Against Domestic & Sexual Violence | Data Safety for Victims of Domestic Violence & their advocates | Portland OR | 40 | Local |
| 84. | Aug-03 | Oklahoma Coalition Against Domestic Violence & Sexual Assault | Technology Use By Abusers, Victims & Their Advocates | Bartlesville OK | 30 | State |
| 85. | Aug-03 | Oklahoma Coalition Against Domestic Violence & Sexual Assault | Data Safety for Victims of Domestic Violence & their advocates | Bartlesville OK | 30 | State |
| 86. | Aug-03 | Oklahoma Coalition Against Domestic Violence & Sexual Assault | Technology Use By Abusers, Victims & Their Advocates | Enid OK | 30 | State |
| 87. | Aug-03 | Oklahoma Coalition Against Domestic Violence & Sexual Assault | Data Safety for Victims of Domestic Violence & their advocates | Enid OK | 30 | State |
| 88. | Aug-03 | Oklahoma Coalition Against Domestic Violence & Sexual Assault | Technology Use By Abusers, Victims & Their Advocates | Shawnee OK | 30 | State |
| 89. | Aug-03 | Oklahoma Coalition Against Domestic Violence & Sexual Assault | Data Safety for Victims of Domestic Violence & their advocates | Shawnee OK | 30 | State |
| 90. | Sep-03 | New York State Department of Children's Services, Office of Victim Services | Technology Use By Abusers, Victims & Their Advocates | Glenn Falls, NY | 120 | State |
| 91. | Sep-03 | New York State Coalition Against Domestic Violence | Technology Use By Abusers, Victims & Their Advocates | Albany, NY | 30 | State |
| 92. | Sep-03 | Coalition Advocates And Attorneys Network | Data Safety for Victims of Domestic Violence & their advocates | Tucson, AZ | 80 | National |
| 93. | Sep-03 | Georgia Coalition Against Domestic Violence | Data Safety for Victims of Domestic Violence & their advocates | Macon, GA | 40 | State |
| 94. | Sep-03 | National College of District Attorneys National Domestic Violence Conference | Intimate Cyberstalking | New Orleans, LA | 300 | National |
| 95. | Sep-03 | Arizona Coalition Against Domestic Violence | Technology Use By Abusers, Victims & Their Advocates | Tucson, AZ | 25 | Local |
| 96. | Oct-03 | Wisconsin Coalition Against Domestic Violence | Technology Use By Abusers, Victims & Their Advocates | Madison, WI | 30 | State |
| 97. | Oct-03 | Wisconsin Coalition Against Domestic Violence | Technology Use By Abusers, Victims & Their Advocates | Madison, WI | 30 | State |
| 98. | Oct-03 | Mary Kay Independent Sales Directors | Technology Use By Abusers, Victims & Their Advocates | Oakton, VA | 50 | Local |

| | Date | Sponsor | Training Topic | Location | # | Type |
|---|---|---|---|---|---|---|
| 99. | Oct-03 | Suited for Change Non-Profit Organization | Technology Use By Abusers, Victims & Their Advocates | Laurel, MD | 30 | Local |
| 100. | Oct-03 | 10th Annual Conference on Domestic Abuse | Technology Use By Abusers, Victims & Their Advocates | Prior Lake, MN | 200 | State |
| 101. | Oct-03 | U.S. Department of Defense, Fleet and Family Support Center, Family Advocacy Program | Technology Use By Abusers, Victims & Their Advocates | Anacostia Naval Station Washington, DC | 50 | Local |
| 102. | Oct-03 | Indiana Coalition Against Domestic Violence | Technology Use By Abusers, Victims & Their Advocates | Indianapolis, IN | 60 | State |
| 103. | Oct-03 | University of Hawaii | Technology Safety for Victims | Honolulu, HI | 10 | Local |
| 104. | Oct-03 | Hawaii Dept of the Attorney General | Technology Use By Abusers, Victims & Their Advocates | Honolulu, HI | 65 | State |
| 105. | Oct-03 | Turning Point, Hawaii Prosecutor, Hawaii Police | Technology Use By Abusers, Victims & Their Advocates | Hilo, HI | 35 | State |
| 106. | Oct-03 | Turning Point, Hawaii Prosecutor, Hawaii Police | Technology Use By Abusers, Victims & Their Advocates | Kona, HI | 40 | State |
| 107. | Nov-03 | National Network to End Domestic Violence Fund National Meeting | Data Safety for Victims of Domestic Violence & their advocates | Miami, FL | 70 | National |
| 108. | Nov-03 | Kauai Police & the YWCA | Stalking & High-Tech Domestic Violence | Lihue, Kauai | 60 | State |
| 109. | Jan-04 | National Network to End Domestic Violence Fund & Stalking Resource Center | The Use of Technology to Stalk in Intimate Violence | Miami, FL | 80 | National |
| 110. | Jan-04 | National Network to End Domestic Violence Fund & Stalking Resource Center | Data Safety for Victims of Domestic Violence & their advocates | Miami, FL | 80 | National |
| 111. | Jan-04 | National Network to End Domestic Violence Fund & Stalking Resource Center | On the Horizon, Technology misuse by stalkers in the near future | Miami, FL | 80 | National |
| 112. | Jan-04 | North Dakota Prosecutors | ND Prosecutors Winter Conference | Bismarck, ND | 60 | State |
| 113. | Jan-04 | North Dakota Prosecutors | ND Prosecutors Winter Conference | Bismarck, ND | 60 | State |
| 114. | Jan-04 | Access to Justice Committee - Technology Values in the Justice System | Conference on Privacy and Access | Seattle, WA | 90 | State |
| 115. | Mar-04 | US Dept of Justice, Office on Violence Against Women | Technology Use By Abusers, Victims & Their Advocates | San Antonio, TX | 200 | National |
| 116. | Mar-04 | US Dept of Justice, Office on Violence Against Women | Data Safety for Victims of Domestic Violence & their advocates | San Antonio, TX | 30 | National |

| | Date | Sponsor | Training Topic | Location | # | Type |
|---|---|---|---|---|---|---|
| 117. | Mar-04 | White Plains Domestic Violence Coalition | Developing Safe Community Data systems | White Plains, NY | 45 | Local |
| 118. | Mar-04 | White Plains Domestic Violence Coalition | Developing Safe Community Data systems | White Plains, NY | 30 | Local |
| 119. | Mar-04 | San Diego Family Justice Center | Data Safety for Victims of Domestic Violence & their advocates | San Diego, CA | 30 | Local |
| 120. | Mar-04 | San Diego Family Justice Center | Technology Use By Abusers, Victims & Their Advocates | San Diego, CA | 40 | Local |
| 121. | Apr-04 | University of Colorado, Graduate School of Public Affairs | Advanced Tech Safety/Data or something for Program on Domestic Violence | Denver, CO | 30 | Local |
| 122. | Apr-04 | University of Colorado, Graduate School of Public Affairs | Data Safety for Victims of Domestic Violence & their advocates | Denver, CO | 60 | Local |
| 123. | Apr-04 | Mary Kay National Sales Directors | Domestic Violence and Safety Net for the Mary Kay, Inc. Sales Force | Dallas, TX | 60 | Local |
| 124. | Apr-04 | Mary Kay | Supporting DV Survivors for Mary Kay Headquarters | Dallas, TX | 30 | National |
| 125. | Apr-04 | Colorado Coalition Against Domestic Violence | Data Safety for Victims of Domestic Violence & their advocates | Denver, CO | 15 | Local |
| 126. | Apr-04 | 16th Annual Conference on Computers, Freedom, and Privacy | Overseeing the Poor: Technology Privacy Invasions of Vulnerable Groups | Berkeley, CA | 300 | National |
| 127. | May-04 | New York State Crime Victims Board Statewide Conference | Technology Use By Abusers, Victims & Their Advocates | Buffalo, NY | 90 | State |
| 128. | May-04 | National Network to End Domestic Violence Fund Safety Net, Training of Trainers v2.0 | Technology Use By Abusers, Victims & Their Advocates | Chicago, IL | 60 | National |
| 129. | May-04 | National Network to End Domestic Violence Fund Safety Net, Training of Trainers v2.0 | Data Safety for Victims of Domestic Violence & their advocates | Chicago, IL | 80 | National |
| 130. | May-04 | National Network to End Domestic Violence Fund Safety Net, Training of Trainers v2.0 | Assistive Technologies and Emerging Technologies | Chicago, IL | 80 | National |
| 131. | May-04 | National Network to End Domestic Violence Fund Safety Net, Training of Trainers v2.0 | Technology Safety Planning | Chicago, IL | 80 | National |
| 132. | Jun-04 | Washington State Coalition Against Domestic Violence & Washington Coalition Against Sexual Assault Programs | Technology Use By Abusers, Victims & Their Advocates | Yakima, WA | 100 | State |

| | Date | Sponsor | Training Topic | Location | # | Type |
|---|---|---|---|---|---|---|
| 133. | Jun-04 | Rhode Island Justice Commission | Technology Use By Abusers, Victims & Their Advocates | Portsmouth, RI | 60 | State |
| 134. | Aug-04 | Domestic Violence Resource Network | Data Safety for Victims of Domestic Violence & their advocates | Teleconference | 15 | National |
| 135. | Aug-04 | Illinois Coalition Against Domestic Violence | Data Safety for Victims of Domestic Violence & their advocates | Teleconference | 10 | State |
| 136. | Aug-04 | President's Family Justice Center Initiative | Data Safety for Victims of Domestic Violence & their advocates | San Diego, CA | 100 | National |
| 137. | Aug-04 | National Resource Center on Domestic Violence | Data Safety for Victims of Domestic Violence & their advocates | Teleconference | 10 | National |
| 138. | Aug-04 | National Network to End Domestic Violence Fund | Data Safety for Victims of Domestic Violence & their advocates | Teleconference | 75 | National |
| 139. | Aug-04 | National Network to End Domestic Violence Fund | Data Safety for Victims of Domestic Violence & their advocates | Teleconference | 20 | National |
| 140. | Aug-04 | Tennessee Coalition Against Sexual and Domestic Violence | Data Safety for Victims of Domestic Violence & their advocates | Teleconference | 21 | State |
| 141. | Sep-04 | Ohio Domestic Violence Network | Data Safety for Victims of Domestic Violence & their advocates | Teleconference | 22 | State |
| 142. | Sep-04 | National Network to End Domestic Violence Fund | Data Safety for Victims of Domestic Violence & their advocates | Teleconference | 346 | National |
| 143. | Sep-04 | Coalition Advocates and Attorneys Network | Data Safety for Victims of Domestic Violence & their advocates | Pittsburgh, PA | 20 | National |
| 144. | Sep-04 | Nevada Network Against Domestic Violence | Data Safety for Victims of Domestic Violence & their advocates | Teleconference | 5 | State |
| 145. | Sep-04 | President's Family Justice Center Initiative | Data Safety for Victims of Domestic Violence & their advocates | Nampa, ID | 8 | Local |
| 146. | Sep-04 | President's Family Justice Center Initiative | Technology Use By Abusers, Victims & Their Advocates | Nampa, ID | 16 | Local |
| 147. | Oct-04 | Ohio Domestic Violence Network | Data Safety for Victims of Domestic Violence & their advocates | Teleconference | 4 | State |

| | Date | Sponsor | Training Topic | Location | # | Type |
|---|---|---|---|---|---|---|
| 148. | Oct-04 | Virginia Sexual and Domestic Violence Action Alliance | Data Safety for Victims of Domestic Violence & their advocates | Teleconference | 15 | State |
| 149. | Oct-04 | US Dept. of Health and Human Services, Family Violence Prevention Services Act | Data Safety for Victims of Domestic Violence & their advocates | Washington, DC | 50 | National |
| 150. | Oct-04 | National Network to End Domestic Violence Fund | Data Safety for Victims of Domestic Violence & their advocates | Teleconference | 45 | National |
| 151. | Oct-04 | National Network to End Domestic Violence Fund | Data Safety for Victims of Domestic Violence & their advocates | Teleconference | 350 | National |
| 152. | Oct-04 | California Alliance Against Domestic Violence | Technology Use By Abusers, Victims & Their Advocates | San Francisco | 90 | State |
| 153. | Oct-04 | Washington State Coalition Against Domestic Violence | Data Safety for Victims of Domestic Violence & their advocates | Teleconference | 20 | State |
| 154. | Oct-04 | California Alliance Against Domestic Violence | Data Safety for Victims of Domestic Violence & their advocates | Teleconference | 15 | State |
| 155. | Nov-04 | National College of District Attorneys National Domestic Violence Conference | Technology Use By Abusers, Victims & Their Advocates | Anaheim, CA | 200 | National |
| 156. | Nov-04 | Iowa Coalition Against Domestic Violence | Data Safety for Victims of Domestic Violence & their advocates | Des Moines, IA | 35 | State |
| 157. | Nov-04 | Iowa Coalition Against Domestic Violence | Data Safety for Victims of Domestic Violence & their advocates | Des Moines, IA | 45 | State |
| 158. | Dec-04 | South Dakota Dept. of Victim Services | Data Safety for Victims of Domestic Violence & their advocates | Teleconference | 20 | State |
| 159. | Dec-04 | National 211 Call | Data Safety for Victims of Domestic Violence & their advocates | Teleconference | 100 | National |
| 160. | Jan-05 | Rhode Island Coalition Against Domestic Violence | Data Safety for Victims of Domestic Violence & their advocates | Providence, RI | 20 | State |
| 161. | Jan-05 | California Alliance Against Domestic Violence | Data Safety for Victims of Domestic Violence & their advocates | Teleconference | 20 | State |
| 162. | Jan-05 | New Mexico State Dept of Children, Youth, and Families | Data Safety for Victims of Domestic Violence & their advocates | Santa Fe, NM | 15 | State |

| | Date | Sponsor | Training Topic | Location | # | Type |
|---|---|---|---|---|---|---|
| 163. | Jan-05 | Alaska State Police | Technology Use By Abusers, Victims & Their Advocates | Anchorage, AK | 65 | State |
| 164. | Feb-05 | National Network to End Domestic Violence Fund | Data Workgroup Training | Topeka, KS | 45 | National |
| 165. | Feb-05 | National Network to End Domestic Violence Fund | Data Workgroup Training | Topeka, KS | 45 | National |
| 166. | Feb-05 | National Center on Domestic and Sexual Violence | Program Development | Austin, TX | 10 | National |
| 167. | Feb-05 | North Dakota Council on Abused Women's Services | Data Safety for Victims of Domestic Violence & their advocates | Teleconference | 20 | State |
| 168. | Feb-05 | Utah Domestic Violence Council | Data Safety for Victims of Domestic Violence & their advocates | Teleconference | 25 | State |
| 169. | Mar-05 | Council of Social Work Education | Technology Use By Abusers, Victims & Their Advocates | New York, NY | 15 | National |
| 170. | Mar-05 | Altria Group, Inc. | Data Safety for Victims of Domestic Violence & their advocates | Washington, DC | 40 | National |
| 171. | Mar-05 | President's Family Justice Center Initiative | Technology Use By Abusers, Victims & Their Advocates | Boston, MA | 40 | Local |
| 172. | Mar-05 | President's Family Justice Center Initiative | Data Safety for Victims of Domestic Violence & their advocates | Boston, MA | 40 | Local |
| 173. | Apr-05 | National Network to End Domestic Violence Fund & Stalking Resource Center | Technology Use By Abusers, Victims & Their Advocates | Seattle, WA | 140 | National |
| 174. | Apr-05 | Washington State Coalition Against Domestic Violence | Data Safety for Victims of Domestic Violence & their advocates | Seattle, WA | 15 | State |
| 175. | Apr-05 | National Network to End Domestic Violence Fund & Stalking Resource Center | Emerging Technologies and their Impact on Victims | Seattle, WA | 140 | National |
| 176. | Apr-05 | President's Family Justice Center Initiative | Technology Use By Abusers, Victims & Their Advocates | San Antonio, TX | 40 | Local |
| 177. | Apr-05 | President's Family Justice Center Initiative | Data Safety for Victims of Domestic Violence & their advocates | San Antonio, TX | 40 | Local |
| 178. | Apr-05 | 15th Annual Conference on Computers, Freedom, and Privacy | Data Mining and Public Records | Seattle, WA | 200 | National |
| 179. | Apr-05 | STOP DV Annual Domestic Violence Conference | Technology Use By Abusers, Victims & Their Advocates | San Diego, CA | 100 | National |

| | Date | Sponsor | Training Topic | Location | # | Type |
|---|---|---|---|---|---|---|
| 180. | May-05 | Colorado Coalition Against Domestic Violence | Data Safety for Victims of Domestic Violence & their advocates | Teleconference | 30 | State |
| 181. | May-05 | Colorado Coalition Against Domestic Violence | Data Safety for Victims of Domestic Violence & their advocates | Teleconference | 35 | State |
| 182. | May-05 | Colorado Coalition Against Domestic Violence | Data Safety for Victims of Domestic Violence & their advocates | Teleconference | 10 | State |
| 183. | May-05 | California Alliance Against Domestic Violence | Data Safety for Victims of Domestic Violence & their advocates | Teleconference | 30 | State |
| 184. | Jun-05 | New Mexico Coalition Against Domestic Violence | Data Safety for Victims of Domestic Violence & their advocates | Santa Fe, NM | 50 | State |
| 185. | Jun-05 | National Network to End Domestic Violence Fund Allstate Economic Justice Conference | Technology Use By Abusers, Victims & Their Advocates | Chicago, IL | 10 | National |
| 186. | Jun-05 | U.S. DOJ Global Justice Extensible Markup Language (XML) Data Model (GJXDM) Conference | What's Privacy Got to Do With It? Technology, Privacy, and Victim Safety | Atlanta, GA | 40 | National |
| 187. | Jun-05 | California Alliance Against Domestic Violence | Data Safety for Victims of Domestic Violence & their advocates | Teleconference | 30 | State |
| 188. | Jun-05 | National Center for Victims of Crime | Technology Use By Abusers, Victims & Their Advocates | Washington, DC | 100 | National |
| 189. | Jun-05 | President's Family Justice Center Initiative | Technology Use By Abusers, Victims & Their Advocates | Monroe, LA | 15 | Local |
| 190. | Jun-05 | President's Family Justice Center Initiative | Data Safety for Victims of Domestic Violence & their advocates | Monroe, LA | 15 | Local |
| 191. | Jul-05 | Kentucky Domestic Violence Association | Data Safety for Victims of Domestic Violence & their advocates | Teleconference | 20 | State |
| 192. | Jul-05 | National Network to End Domestic Violence Fund Safety Net, Training of Trainers v3.0 | Data Safety for Victims of Domestic Violence & their advocates | Teleconference | 15 | National |
| 193. | Jul-05 | National Network to End Domestic Violence Fund Safety Net, Training of Trainers v3.0 | Privacy and Technology: The Impact on Victim Safety | San Jose, CA | 90 | National |
| 194. | Jul-05 | National Network to End Domestic Violence Fund Safety Net, Training of Trainers v3.0 | Technology Use By Abusers, Victims & Their Advocates | San Jose, CA | 90 | National |

| | Date | Sponsor | Training Topic | Location | # | Type |
|---|---|---|---|---|---|---|
| 195. | Jul-05 | National Network to End Domestic Violence Fund Safety Net, Training of Trainers v3.0 | Data Safety for Victims of Domestic Violence & their advocates | San Jose, CA | 90 | National |
| 196. | Jul-05 | National Network to End Domestic Violence Fund Safety Net, Training of Trainers v3.0 | Emerging Technologies and their Impact on Victims | San Jose, CA | 75 | National |
| 197. | Jul-05 | New Mexico Coalition Against Domestic Violence | Data Safety for Victims of Domestic Violence & their advocates | Teleconference | 15 | State |
| 198. | Jul-05 | New Mexico Coalition Against Domestic Violence | Data Safety for Victims of Domestic Violence & their advocates | Teleconference | 10 | State |
| 199. | Aug-05 | US Dept. of Health and Human Services, Family Violence Prevention Services Act | Data Safety for Victims of Domestic Violence & their advocates | St Louis, MO | 60 | National |
| 200. | Sep-05 | President's Family Justice Center Initiative | Community Based Organizations Working for Victim Safety | Tulsa, OK | 10 | Local |
| 201. | Sep-05 | President's Family Justice Center Initiative | Technology Use By Abusers, Victims & Their Advocates | Tulsa, OK | 25 | Local |
| 202. | Sep-05 | President's Family Justice Center Initiative | Data Safety for Victims of Domestic Violence & their advocates | Tulsa, OK | 20 | Local |
| 203. | Oct-05 | President's Family Justice Center Initiative | Community Based Organizations Working for Victim Safety | Tampa, FL | 10 | Local |
| 204. | Oct-05 | President's Family Justice Center Initiative | Technology Use By Abusers, Victims & Their Advocates | Tampa, FL | 20 | Local |
| 205. | Oct-05 | Ending Violence Against Women International | High-Tech Violence Against Women | Baltimore, MD | 300 | National |
| 206. | Oct-05 | Local Domestic Violence Task Force | Technology Use By Abusers, Victims & Their Advocates | Frederick, MD | 150 | Local |
| 207. | Oct-05 | National College of District Attorneys National Domestic Violence Conference | Technology Use By Abusers, Victims & Their Advocates | Reno, NV | 50 | National |
| 208. | Oct-05 | President's Family Justice Center Initiative | Data Safety for Victims of Domestic Violence & their advocates | Tampa, FL | 15 | Local |
| 209. | Nov-05 | Bureau of Justice Assistance, Technology Privacy Focus Group | Privacy and Technology: The Impact on Victim Safety | Phoenix, AZ | 50 | National |
| 210. | Dec-05 | US Dept of Health and Human Services, Office of Community Services | Data Safety for Victims of Domestic Violence & their advocates | Teleconference | 15 | National |

| | Date | Sponsor | Training Topic | Location | # | Type |
|---|---|---|---|---|---|---|
| 211. | Dec-05 | Women Against Violence Europe | Technology Use By Abusers, Victims & Their Advocates | Copenhagen, DK | 45 | Intl |
| 212. | Feb-06 | National Network to End Domestic Violence Fund | National Training Call | Teleconference | 80 | National |
| 213. | Feb-06 | National Network to End Domestic Violence Fund | National Training Call | Teleconference | 600 | National |
| 214. | Feb-06 | US Dept. of Health and Human Services, Family Violence Prevention Services Act Grant Administrators | Data Safety for Victims of Domestic Violence & their advocates | Salem, OR | 40 | State |
| 215. | Feb-06 | National Network to End Domestic Violence Fund | Data Safety for Victims of Domestic Violence & their advocates | Teleconference | 30 | National |
| 216. | Feb-06 | Michigan Coalition Against Domestic and Sexual Violence | Data Safety for Victims of Domestic Violence & their advocates | Teleconference | 30 | State |
| 217. | Feb-06 | Anti-Spyware Coalition Public Workshop: Defining the Problem, Developing Solutions | Spyware's Impact on Businesses and Individuals | Washington, DC | 300 | Intl |
| 218. | Mar-06 | Jewish Women International | Data Safety for Victims of Domestic Violence & their advocates | Teleconference | 75 | National |
| 219. | Mar-06 | US Dept. of Health and Human Services, Family Violence Prevention Services Act | Data Safety for Victims of Domestic Violence & their advocates | St Louis, MO | 40 | National |
| 220. | Mar-06 | Fairfax County Domestic Violence Task Force | Technology Use By Abusers, Victims & Their Advocates | Fairfax, VA | 45 | Local |
| 221. | Mar-06 | University of New England, School of Social Work | Data Safety for Victims of Domestic Violence & their advocates | Portland, ME | 30 | Local |
| 222. | Mar-06 | University of Southern Maine, Muskie School of Public Service | Technology, Stalking, Data Safety for Victims of Domestic Violence & their advocates | Portland, ME | 30 | National |
| 223. | Mar-06 | Women Against Violence Europe | Capacity and Development | New York, NY | 5 | Intl |
| 224. | Apr-06 | National Association of Attorneys General | Technology Use By Abusers, Victims & Their Advocates | Oxford, MS | 60 | National |
| 225. | Apr-06 | Quantico Marine Base Family Advocacy Program | Youth and Internet Safety | Quantico, VA | 50 | Local |
| 226. | Apr-06 | New Mexico Coalition Against Domestic Violence | Data Safety for Victims of Domestic Violence & their advocates | Teleconference | 30 | State |
| 227. | Apr-06 | Mary Kay | Domestic Violence 101 | Reston, VA | 25 | Local |

| | Date | Sponsor | Training Topic | Location | # | Type |
|---|---|---|---|---|---|---|
| 228. | Apr-06 | CA Administrative Office of the Courts (AOC), Center for Families, Children & the Courts (CFCC) | Technology Use By Abusers, Victims & Their Advocates | Los Angeles, CA | 100 | State |
| 229. | Apr-06 | CA Administrative Office of the Courts (AOC), Center for Families, Children & the Courts (CFCC) | Data Safety for Victims of Domestic Violence & their advocates | Los Angeles, CA | 100 | State |
| 230. | May-06 | 16th Annual Conference on Computers, Freedom, and Privacy | Technology& Privacy Impacts on Hurricane Evacuees | Washington, DC | 250 | National |
| 231. | May-06 | Florida Coalition Against Domestic Violence | Data Safety for Victims of Domestic Violence & their advocates | Teleconference | 10 | State |
| 232. | May-06 | National Network to End Domestic Violence Fund | Protection Order Registries | Teleconference | 5 | State |
| 233. | May-06 | Anti-Spyware Coalition | SpyWare and its Misuses | Ottawa, CA | 200 | Intl |
| 234. | May-06 | Ottawa Dept. of Justice | Technology Use By Abusers, Victims & Their Advocates | Ottawa, CA | 5 | Intl |
| 235. | May-06 | Ottawa Dept. of Health | Technology Use By Abusers, Victims & Their Advocates | Ottawa, CA | 5 | Intl |
| 236. | May-06 | Ottawa Privacy Commission | Technology Use By Abusers, Victims & Their Advocates | Ottawa, CA | 40 | Intl |
| 237. | May-06 | Canadian Internet Policy and Public Interest Clinic, Ottawa University | Technology Use By Abusers, Victims & Their Advocates | Ottawa, CA | 40 | Intl |
| 238. | May-06 | Texas Municipal Police Association, Sexual Assault and Family Violence Investigator's Course | Technology Use By Abusers, Victims & Their Advocates | San Antonio, TX | 90 | State |
| 239. | Jun-06 | Florida Coalition Against Domestic Violence | Data Safety for Victims of Domestic Violence & their advocates | Teleconference | 15 | State |
| 240. | Jun-06 | America Online | Technology Use By Abusers, Victims & Their Advocates | Dulles, VA | 30 | Local |
| 241. | Jul-06 | National Coalition Against Domestic Violence | Confidentiality and Data Safety for Victims of Domestic Violence & their advocates | Atlanta, GA | 40 | National |
| 242. | Jul-06 | US Dept. of Justice, Office of Violence Against Women, Office of Rural Grantees | Technology Use By Abusers, Victims & Their Advocates | Teleconference | 40 | Nation |

| | Date | Sponsor | Training Topic | Location | # | Type |
|---|---|---|---|---|---|---|
| 243. | Jul-06 | US Dept. of Health and Human Services, Family Violence Prevention Services Act | Confidentiality and Data Safety for Victims of Domestic Violence & their advocates | St Louis, MO | 70 | National |
| 244. | Jul-06 | US Dept. of Health and Human Services, Family Violence Prevention Services Act Grant Administrators | Confidentiality and Data Safety for Victims of Domestic Violence & their advocates | St Louis, MO | 60 | National |
| 245. | Aug-06 | National Network to End Domestic Violence Fund Safety Net, Training of Trainers v4.0 | Technology Use By Abusers, Victims & Their Advocates | Indianapolis | 90 | National |
| 246. | Aug-06 | National Network to End Domestic Violence Fund Safety Net, Training of Trainers v4.0 | Technology Use By Abusers, Victims & Their Advocates | Indianapolis | 90 | National |
| 247. | Aug-06 | National Network to End Domestic Violence Fund Safety Net, Training of Trainers v4.0 | Technology Use By Abusers, Victims & Their Advocates | Indianapolis | 90 | National |
| 248. | Aug-06 | National Network to End Domestic Violence Fund Safety Net, Training of Trainers v4.0 | Technology Use By Abusers, Victims & Their Advocates | Indianapolis | 75 | National |
| 249. | Aug-06 | National Network to End Domestic Violence Fund | Data Safety for Victims of Domestic Violence & their advocates | Teleconference | 45 | National |
| 250. | Sep-06 | Wyoming Dept. of Victim Services | Use of Technology in Stalking | Jackson Hole, WY | 150 | State |
| 251. | Sep-06 | Wyoming Dept. of Victim Services | Technology's Impact on Survivor Safety | Jackson Hole, WY | 30 | State |
| 252. | Sep-06 | National Network to End Domestic Violence Fund & Stalking Resource Center | Technology Use By Abusers, Victims & Their Advocates | Minneapolis, MN | 100 | National |
| 253. | Sep-06 | National Network to End Domestic Violence Fund & Stalking Resource Center | Advanced Safety Planning | Minneapolis, MN | 40 | National |
| 254. | Sep-06 | National Network to End Domestic Violence Fund & Stalking Resource Center | Emerging Technologies and their Impact on Victims | Minneapolis, MN | 100 | National |
| 255. | Oct-06 | President's Family Justice Center Initiative | Community Based Organizations Working for Victim Safety | South Bend, IN | 8 | Local |
| 256. | Oct-06 | President's Family Justice Center Initiative | Technology Use By Abusers, Victims & Their Advocates | South Bend, IN | 50 | Local |
| 257. | Oct-06 | President's Family Justice Center Initiative | Data Safety for Victims of Domestic Violence & their advocates | South Bend, IN | 45 | Local |

| | Date | Sponsor | Training Topic | Location | # | Type |
|---|---|---|---|---|---|---|
| 258. | Oct-06 | Women Against Violence Europe | Strategies for creating partners to focus on technology and abuse | Lisbon, Portugal | 45 | Intl |
| 259. | Nov-06 | Verizon National Domestic Violence Summit | Applications of technology relating to victims of domestic violence | Basking Ridge, NJ | 100 | National |
| | | | | | 14,885 | |

# PLAINTIFFS' RULE 26(a)(2) EXPERT WITNESS REPORT OF EVAN HENDRICKS

I, Evan Hendricks, provide the following Expert Report pursuant to Federal Rules of Civil Procedure 26(a)(2) in connection with the action entitled Federal Trade Commission vs. Accusearch, Inc., et al., U.S. District Court for the District of Wyoming, Case No. 06CV0105-D. If appropriate, and if justified by the production of additional evidence in discovery, I reserve the right to supplement this report at a future date. My qualifications and CV are at the end of this report, beginning on page 30.

The Federal Trade Commission (FTC) has retained me to address the following questions:

1. Does the practice of obtaining and selling a consumer's personal telephone records without that consumer's permission cause harm to such consumers or to third parties? If so, please describe the types of harms that are caused or likely to be caused, the extent of such harm, and whether the consumers or third parties can take steps to avoid suffering the harm.

2. Please describe any countervailing benefits that result from the practice of obtaining and selling a consumer's personal telephone records without that consumer's permission.

3. Please review the steps AccuSearch alleges it takes to ensure that it releases information only for appropriate purposes, as those steps are described in AccuSearch's Brief in Support of Defendant's Motion to Dismiss Complaint for Injunctive and Other Relief, Defendants' Responses to Plaintiff's First Interrogatories (omitting Exhibit A), and Defendants' Supplemental Responses to Plaintiff's First Set of Interrogatories. Are those steps sufficient to avoid or mitigate any harm that may come to consumers from

having their telephone records sold without their permission? What steps, if any, would be sufficient?

**I will proceed by answering each question, and cite to later sections in this report that support and explain my opinions.**

1. Does the practice of obtaining and selling a consumer's personal telephone records without that consumer's permission cause harm to such consumers or to third parties? If so, please describe the types of harms that are caused or likely to be caused, the extent of such harm, and whether the consumers or third parties can take steps to avoid suffering the harm.

**Response:** The data brokers' practice of obtaining and selling consumer's phone calling records, which virtually in all cases are obtained by using underhanded means as pretexts, bribes or hacking, which by definition means that it is happening without the consumer's consent, causes several specific and general harms to consumers, including (but not limited to) the following:

- Individuals who learn that their cell phone calling records were compromised by the fraudulent tactics of data brokers consistently describe it as a gross invasion of their privacy. The oft-repeated statement that they "feel violated," relates directly to the vernacular used by privacy experts to describe such incidents: this is "data rape," pure and simple. Medical professionals have found that victims of such privacy invasions often suffer from Post Traumatic Stress Syndrome.[1] (For example, see below "Case Studies" section, Congressional testimony of Journalist Christopher Byron, and in the "History" section, comments of Oprah Winfrey.)

[1] "Identity Theft: The Aftermath 2003," Identity Theft Resource Center (Sept. 2003); see findings of Dr. Charles Nelson, a licensed psychologist, and director of both the Crime and Trauma Recovery Program at the Family Treatment Institute; http://www.idtheftcenter.org/aftermath.pdf

- A data broker who is obtaining the victim's phone records by way of underhanded means is doing so because the broker has a paying client that is either seeking to take serious, adverse action against the victim, or investigating whether or not to do so. (See "Case Studies" section; also see Defendant's invoices and emails). Thus, by definition, the use of pretexts or bribes to obtain a consumer's phone records involves harm or potential harm to that consumer.
- These tactics can cause "collateral" damage to the privacy of people who are related to the target of a data brokers' efforts, as data about them are reflected in the calling records of the target. (See "Case Studies" section; also see Defendant's invoices and emails.) If the data broker or investigator is aggressive, he may choose to obtain the records of these third parties as well.
- Data brokers' tactics are forcing phone companies to incur additional costs that assuredly will be passed on to consumers. Moreover, the evolving safeguards are making it more inconvenient for consumers to gain access to their own records for legitimate, routine purposes. (See "Wireless Phone Companies" section.)
- Another concern is the potential harm to confidential relationships. As the testimony of Mr. Byron made clear, phone records can help expose a journalist's confidential sources. The same is true of confidential relationships between therapists or doctors and patients, attorneys and clients, members of the clergy and their parishioners, and the like.
- The general threat posed by unethical data brokers creates a general feeling of insecurity that Americans are losing reasonable control over their personal information. This concern has been identified repeatedly in opinion polls and by leading research studies. For instance, in 1981, the Congressional Office of Technology Assessment (OTA), observed that highly invasive and unreasonable data practices, such as those used by data brokers, "may increase suspicion some citizens

have of large organizations – business, labor or government – and thus erode cooperation and a personal sense of well-being."[2]

**Question 2:** Please describe any countervailing benefits that result from the practice of obtaining and selling a consumer's personal telephone records without that consumer's permission.

**Response:** The only indications of "countervailing benefits" are the sporadic, but sometimes unsubstantiated claims of data brokers that their actions help locate witnesses for litigation, or debtors or people who skipped out on their bail bonds. Consequently, some data brokers imply that their *means*, use of pretexts and bribes, are justified by these ends.

However, in most, if not all of these contexts, our judicial process offers an established method for the discovery of documents that are relevant to any given case: the subpoena.

Once a party shows that information is relevant, they have broad rights to subpoena that information. Protections are built in, as the target of the subpoena often has the right and opportunity to show that the records are not relevant, and thereby prevent their disclosure to a hostile party. The decision appropriately is made by a neutral third party – a magistrate or judge. Moreover, a magistrate or judge can provide further protection when necessary by placing restrictions on the recipients' use of subpoenaed information, or otherwise placing it under a protective order. The process is consistent with the Fair Information Practice (FIPs) standards discussed below.

Pretexts and bribes, on the hand, reflect contempt for the well-established subpoena process and violate FIPs. They are a convenient and time-saving shortcut for those that have the means and inclination to pay for such tactics.

[2] "Computer-Based National Information Systems," Office of Technology Assessment (1981)

Despite the volume handled by some data brokers, their number of cases pale in comparison to the number of law-abiding Americans who have cell phones. According to their recent Congressional testimony or company Web sites, below are estimates of numbers of customers:

- Verizon – 54 million
- Cingular – 58 million
- Sprint – 50 million "plus"
- T-Mobile – 24 million
- Alltell – 11 million

In my opinion, the importance of protecting the privacy and security of the cell phone records of some 150 million Americans clearly outweighs the interests of a relatively small community of data brokers that use fraudulent means to surreptitiously obtain the records of thousands of consumers.

**Question 3:** Please review the steps AccuSearch alleges it takes to ensure that it releases information only for appropriate purposes, as those steps are described in AccuSearch's Brief in Support of Defendant's Motion to Dismiss Complaint for Injunctive and Other Relief, Defendants' Responses to Plaintiff's First Interrogatories (omitting Exhibit A), and Defendants' Supplemental Responses to Plaintiff's First Set of Interrogatories. Are those steps sufficient to avoid or mitigate any harm that may come to consumers from having their telephone records sold without their permission? What steps, if any, would be sufficient?

**Response:** AccuSearch's alleged steps to "ensure that it release information only for appropriate purposes" or "to avoid or mitigate any harm that may come to consumers" are entirely inadequate, in my opinion.

The first reason is that a data broker's act of obtaining a consumer's cell phone records, using such fraudulent means as pretexts or bribes, naturally without the consumer's consent, is harmful because it constitutes an unwarranted invasion of privacy, as defined by commonly accepted notions of privacy as defined by standards of Fair Information Practices (FIPs) articulated long ago. (See discussion of FIPs below). AccuSearch's "steps" are inadequate because instead of deterring this invasive act, they are based on the presumption that the invasive act will occur.

Second, the "FAQs" at Defendant's Web site explicitly stated that Defendant did not know whether its "researchers" who actually obtained records used pretext, bribes or other fraudulent practices. The evidence in this case showed that at its Abika.com Web site, Defendant said in its "FAQs" that it connects "searchers" with researchers. "These are independent researchers and *Abika.com does not know how they do the research.* Abika.com notifies researchers who provide non-internet research to only fulfill the research request if they can conduct the research in compliance with Federal, State or Local Laws ..."[3] [Emphasis added]

If Defendant did not know how its researchers did their research, how did Defendant know all of the tactics they used were legal? Moreover, I have seen no evidence in this case that Defendant sought an independent and objective legal analysis of the legality of facilitating the use of pretexts and bribes to obtain confidential cell phone calling records.

Third, orders and invoices produced by Defendant do not indicate whether records were not obtained using pretexts or bribes, thereby supporting the likelihood that they were. Moreover, they not only fail to confirm that records were obtained for a legitimate purpose, they do not indicate any purpose whatsoever.

For example, an order processed and apparently fulfilled by Defendant from "Double Helix," a data broker, entitled, "Re: 48574 - Cell phone activity by billing cycle - $90."

[3] www.abika.com/faqs.htm; visited July 12, 2005

The target of the search is a man who we will refer to by his initials, "M.R.," to ensure privacy. Born in 1977, MR is described as an "ACC Police Officer" living in Athens, Georgia. The "additional information" section of the order form states:

> 1) i want the last completed cell phone bill which includes the date 10-25-05. 2.) i also want the 1st completed cell phone bill which should start 8-16-05.

The attached PDF records of phone bill records for those two months indicated the order was fulfilled.

The order did not indicate what the "searcher's" purpose was, or why he or she needed MR's cell phone calling records. The fact that MR was a police officer should have raised some concerns about the purpose, in my opinion. It is possible that the searcher was an ex-wife trying to collect child support, or a suspicious wife trying to determine if MR was calling another woman, or a debt collector, or a process server. However, in each of these scenarios, the "searcher" could use legitimate and straightforward means of obtaining records, and would not be compelled to turn to a method that necessitates such fraudulent techniques as pretexts or bribes. On the other hand, it is possible that the "searcher" was involved with criminal activity or connected to someone who was involved in such activity, and wanted the information so he or she could take adverse action against MR. What is particularly important here is that, according to the evidence produced by Defendant, even in the case of a police officer, Defendant took no additional steps to ensure that his confidential cell phone calling records were obtained in an ethical manner or would not end up in the hands of a criminal intent on doing him harm. In my opinion, this example strongly supports my view that Defendant's "steps" were woefully inadequate to ensure that consumers' cell phone records were obtained in an ethical manner, or obtained by honorable persons, or would be used for permissible purposes.

As for the "researcher," Double Helix, there were several reasons to be concerned that it was the type of data broker that would use such fraudulent techniques as pretexts or bribes. First, the kind of records it obtains, beginning with cell phone calling records or location information revealed by cell phones, generally require the use of such fraudulent techniques as pretexts or bribes.

Second, at the company's Web site's section entitled, "privacy policy," it asserts that:

> **Double Helix Privacy Policy**
> Double Helix, Inc. operates under IRSG Principles and will follow all Federal, State, and Local policies and procedures in regards to privacy, information retrieval, and disclosure of said information.[4]

Double Helix's page on "privacy policy" next mentions the Gramm-Leach-Bliley Act (GLB). Amazingly, however, the page only notes the duty of banks and insurers to disclose their privacy policies, and makes no mention of GLB's explicit ban on the use of pretexts to obtain customer financial information. The page also does not mention that banks and insurers must adopt safeguards to prevent wrongful disclosure or misuse of customer information. Similarly, the page's next paragraph references the Fair Credit Reporting Act, but nowhere mentions that a potential user of a credit report, including Double Helix, must have a "permissible purpose" to obtain a consumer's report.[5]

The fact that Double Helix fails to mention the privacy provisions of the GLB and the FCRA that are most relevant to its own operations indicates a disregard for these provision, lessening the likelihood that Double Helix would comply with these provisions, in my opinion. Defendant has not produced any evidence to show that it even considered the dubious qualities of a broker like Double Helix.

---

[4] http://www.doublehelixinc.net/privacy.html, visited November 19, 2006
[5] *Id.*

In addition, Double Helix's "FAQ 4" reads:

> How can I determine if I have a permissible purpose for an investigation?
>
> The best bet is to send you (sic) case specifics to us and let us make that decision.[6]

This FAQ presents an opportunity for Double Helix to educate potential customers about the true meaning of "permissible purpose," thereby enabling the customer to determine that paying a third party to use fraudulent techniques such as pretexts or bribes to obtain confidential cell phone calling records is at a minimum, unethical, and at worst, illegal. However, Double Helix squanders this opportunity, by minimizing the importance of the issue and by urging the prospective customer to let Double Helix make the decision.

In Interrogatory No. 10, the FTC asked Defendant to "describe in detail all procedures, criteria, and steps taken by you, if any, to determine the purpose of any customer who sought to purchase consumer phone records from you. Identify all documents relevant to, or used to formulate, your response to this interrogatory."

Defendant's response sidestepped answering the question as to how *it determined the purpose of any customer* who sought to purchase phone records, and instead responded by stating that "Abika.com uses the following *screening process*: ..." [Emphasis added] Its response featured 20 numbered sentences. However, many of these sentences were filled with generalities about ensuring that the person buying the records, the "searcher," seemed suitable to sell confidential records to. These responses avoided the more fundamental issue that the "searcher" was attempting to purchase these records via Defendant because the records were confidential, and therefore could only be obtained in the desired timeframe through the underhanded tactics facilitated by the Defendant. Defendant's responses speak of "suspicious" actions or "suspicious" searchers, but such platitudes are based upon the incorrect assumption

[6] [illegible], visited November 19, 2006

that it is not harmful to consumers or otherwise permissible to obtain cell phone calling records through fraudulent tactics. As the 2005 complaint by the Electronic Privacy Information Center (EPIC) pointed out, the only way to obtain cell phone records in the manner offered by Defendant was through the use of such tactics. Therefore, Defendant's response to Interrogatory No. 10 did not offer adequate safeguards to ensure that cell phone records are only obtained in a fair and permissible manner.

Another reason to doubt the effectiveness of AccuSearch's "steps" is the well-recognized practice among data brokers to prioritize the sale of data over the purpose for which it will be used. Robert Douglas, a private investigator who has closely investigated and tested the practices of data brokers using pretexts and bribes, testified:

> ... [T]oday there are hundreds of ads on the web (and in legal and investigative trade journals) for phone records and phone "research". And contrary to the language on those sites claiming to limit sales of personal information to attorneys; investigators; skip tracers; debt collectors; and, bail bondsmen, most of these companies will sell to anyone as long as they think you're not a reporter or law enforcement agency conducting a media expose or sting operation. Frankly, greed is the name of the game.[7]

John Aravosis, a Washington, D.C.-based blogger demonstrated the ease of obtaining cell phone records without specifying any legitimate purpose, when he posted on www.blogger.com, that he was able to purchase the cell phone calling records of Retired General Wesley Clark for $89.95 from CellTolls via the company's Web site (www.celltolls.com). Without identifying

[7] Testimony of Robert Douglas, House Committee on Energy & Commerce, Hearing on "Phone Records for Sale: Why Aren't Phone Records Safe from Pretexting?" February 1, 2006; http://energycommerce.house.gov/108/Hearings/02012006hearing1756/Douglas.pdf, at 4.

himself to CellTolls, he previously had purchased his own cell phone calling records from LocateCell for $110.[8]

Moreover, in my opinion, the underlying records in the FTC's 2001 "Operation Pretext Detect" will support the view that data brokers generally do not ensure that the tactics for obtaining confidential data are legal or fair, and that brokers do little, if anything, to ensure that the sale of the information is legal or for an acceptable purpose.

**Brief History**

It has been known for some time that private detectives and the like have been able to obtain confidential consumer information using such underhanded means as pretexting and bribing.

In Your Right To Privacy (2nd Edition, Southern Illinois University Press, 1990), a book I co-authored, I devoted a chapter to the issue, entitled "The Wild Card: Private Detectives." The chapter, which featured a question-and-answer format, included the following passage:

> What kind of data can private investigators gain access to?
>
> All kinds, and that's the point. An informal survey of a representative sample of private investigators confirmed what most people already believe to be the case: private investigators can find almost any information they want, regardless of privacy laws or any other security measures. One private investigator, who asks that his name be withheld, said, "If there's enough money you can get anything. You have to find the weak link in the chain and go for it!" "I've never heard of a record I couldn't get if I put my mind to it," said another investigator who also requests anonymity.

[8] http://[illegible].blogspot.com/[illegible]; Aravosis blogged as "John in D.C."

> In fact, no investigator interviewed seemed troubled about disclosure restrictions imposed by various privacy laws. They describe why no record was virtually beyond their reach; "It's all based on contacts," explained on investigator who has experience in federal law enforcement and congressional and private sector security. He added, "Law enforcement officials and former law enforcers who become private investigators form a loose-knit fraternity. Those with a law enforcement background have instant credibility. Federal agents usually have contacts at the state level, who, in turn have contacts at the local level … Private eyes working outside their network must find a colleague to refer him to the proper source – usually another private investigator – and then 'subcontract' with him to get the information you need."

**Indictment of the Data Brokers**

In the years immediately following the book's release, it became readily apparent that private detectives increasingly were relying on a new breed of specialist – the information broker or data broker. The data broker specialized in obtaining, often by way of underhanded tactics, the confidential personal records of the individual who the private investigator was probing. As illustrated below, increased attention paid to data brokers by public officials, law enforcers, the media and the public underscored that Americans considered brokers' use of such underhanded tactics as bribing and pretexting to be highly objectionable, unfair and an invasion of accepted notions of privacy.

- On December 18, 1991, then-U.S. Attorneys Michael Chertoff (Newark, NJ) and Robert Genzman (Tampa, Fla.) announced the indictment of eight information brokers in five states, three Social Security Administration (SSA) employees and five

other individuals in connection with the illegal sale, purchase and/or collection of confidential personal data stored in FBI and SSA computers.[9]

- On February, 28, 1992, the Senate Finance Subcommittee on Social Security held a hearing, further publicizing the threat to privacy posed by data brokers. The comments of then Chairman Sen. Patrick Moynihan, and the testimony of witnesses representing the SSA, FBI, the ACLU and Computer Professionals for Social Responsibility (CPSR) unanimously portrayed the underhanded tactics used by the indicted brokers as highly objectionable, unfair and an invasion of accepted notions of privacy.[10]
- In July 1992, then-U.S. Attorney Chertoff announced the indictment of former HHS Midwest Region Inspector General James Bailey, for allegedly conspiring with already-indicted data broker Al Schweitzer to bribe an SSA employee for confidential earnings data. Meanwhile, the employee, Patricia Rosemond, a special agent in the HHS IG Midwest office, pleaded guilty to conspiracy to commit bribery. Moreover, two other SSA employees, and data brokers, Ned and Susan Fleming, of Super Bureau of Salinas, Calif., also entered guilty pleas. "A person's right to privacy should not be bought or bartered," Chertoff told the media.[11]
- In August 1992, a new book, Privacy For Sale: How Computerization Has Made Everyone's Private Life an Open Secret (Simon & Schuster), catalogued the threat to privacy posed by data brokers, publishing a "price list" in which a data broker using a pseudonym sold individual tax records for the past three years for $500, phone toll records (past 60 days) $200; bank account and balances, or contents of safety deposit boxes – $200. Author Jeffrey Rothfeder garnered publicity for the book by obtaining

---

[9] "HHS Gumshoes Crack Ring of Personal Data Traffickers," *Privacy Times*, Vol.11 No. 23, Dec. 31, 1991.
[10] "Protecting the Privacy of Social Security Numbers and Records," Senate Finance Subcommittee on Social Security and Family Policy, Senate, February 28, 1992;
"Illegal Personal Data Sales Call for Privacy Act, SSN Changes, Experts Say," *Privacy Times*, Vol.12 No. 5, March 11, 1992. (I also testified as an invited witness at the hearing.)
[11] "Info Broker Probe Continues With Indictment of Ex-IG, Special Agent," *Privacy Times*, Vol.12 No. 15, July 30, 1992.

the credit reports of then Vice President Dan Quayle and CBS News Anchor Dan Rather.[12]

- In September 1992, former HHS IG Bailey, and data brokers Al and Petra Schweitzer, pleaded guilty to conspiring to commit bribery in connection with their attempts to compromise SSA records.[13]
- In November 1992, Schweitzer appeared as the lead guest on the Oprah Winfrey Show, explaining that he served a wide variety of clients, attorneys in litigation seeking witnesses or assets, private investigators and collection departments. Schweitzer's appearance was particularly compelling because of his work on behalf of another client, *The National Inquirer*, a tabloid that specialized in reporting gossip about celebrities. As one of his *Inquirer* projects, Schweitzer was tasked with obtaining Ms. Winfrey's unlisted phone number so the tabloid could call her apartment and quiz her chef about her new diet. Sitting one on one with Ms. Winfrey on her show, Schweitzer explained that to obtain her number, Schweitzer had to trick a phone company representative into giving him all of the phone numbers of individuals on the floor in her apartment building. He was then able to narrow the list down to Ms. Winfrey's number. Schweitzer went on to describe his work more generally. Ms. Winfrey told Schweitzer in no uncertain terms that she found his work invasive and highly objectionable and that she felt violated knowing in particular that he had so easily obtained her records and knowing generally that such sensitive personal records were so easily compromised. The audience also communicated its displeasure through its pointed questioning of Schweitzer, and by booing him when he told Winfrey that he was "proud" of his work.

[12] "Privacy Book Review: Rothfeder Goes Underground For Victims, Invaders," *Privacy Times*, Vol.12 No. 16, August 21, 1992.
[13] "Former HHS IG, Two Info Brokers Latest to Plead Guilty in N.J.," *Privacy Times*, Vol.12 No. 17, September 14, 1992.

- In a published interview in *Playboy Magazine*, Schweitzer discussed in detail the inner workings of the data broker industry, which Federal prosecutors said he pioneered. He described many of the "pretexts" or gags he used to get unlisted phone numbers, toll records, credit card charges, bank account information, utility bills and wage data. He worked fast and sold cheap. "I could have your phone number in three minutes and sell it for $50. I could have your phone bill within the hour and sell it for a hundred and a half, no matter how big it was. Your credit card charges, I'd have in minutes," Schweitzer told *Playboy*. He claimed he grossed over $800,000 in 1988.[14]

**Al Schweitzer**

After meeting Schweitzer on the show, I spent considerable time de-briefing him on the nature and scope of his work. He said that for the most part, he could obtain any "confidential" record, provided that there was sufficient time and resources. The list included phone records, various types of financial records, employment records and criminal records.

Schweitzer emphasized that phone records were particularly valuable because they revealed with whom the subject was communicating, and with what frequency, and at what time. His principle methods of obtaining confidential records were through pretexting, or through development of sources inside companies, most of whom he had to bribe. Specifically, he said that he would develop a source in the phone company by going to the employee parking lot and find the least appealing automobile, take down the license plate number, and then obtain the driver's information from the Dept. of Motor Vehicles. His approach was rather simple, telling the phone company employee that his jalopy indicated that he could probably use some extra money, and then asking, "How would you like to earn some selling me phone records?"

[14] "Professional Privacy Invader Could Get Any Personal Record," *Privacy Times*, Vol.13 No. 6, April 1, 1993.

Schweitzer also remarked that selling confidential personal data was much like selling drugs, in the sense that when the "heat was on" (i.e., enforcement was active), the price of personal data went up. He also expressed his opinion that selling personal data was better than selling drugs because it was more lucrative and less risky.

**Gramm-Leach-Bliley Act**

In 1997-98, Massachusetts Attorney General Scott Harshbarger filed civil lawsuits against nine data brokers over their use of underhanded tactics such as bribing and pretexting to obtain confidential records. These actions increased public awareness about unethical data brokers, heightened public outrage just as Congress was considering comprehensive legislation for the financial services industry.

Harshbarger testified at a key committee hearing that ultimately resulted in restrictions on pretexting of financial data, as well as data security safeguards. "While no Massachusetts statute specifically prohibits the buying and selling of private financial information, anyone who repeatedly makes false statements to financial institutions to trick them out of something of value should not be surprised that such conduct runs afoul of the law," he testified, explaining why he did not wait for a federal statute.[15]

At the same House Committee Hearing, Robert Douglas, a private investigator who supported restrictions on obtaining confidential records, Mr. Schweitzer and I also warned that brokers were obtaining using fraudulent techniques to obtain other confidential records, including phone calling records.

> The threat to privacy of Americans posed by the so-called "Information Broker" industry is probably the most serious of a variety of threats that exist in

[15] Testimony of Scott Harshbarger, Attorney General of the Commonwealth of Massachusetts, House Committee on Banking and Financial Services, July 28, 1998 (Delivered by Assistant Attorney General Jeffrey D. Clements)

> the rapidly-changing Information Age. When the price is right, information brokers usually can get an individual's most sensitive personal data, including bank, credit card, telephone, medical, pharmacy, travel, employment and government records. This astonishing ability rightfully frightens the overwhelming majority of Americans who are concerned about threats to their privacy. It makes a mockery out the existing patchwork of consumer privacy laws and underscores the need for broad-based legislation that will give consumers the privacy rights they deserve.[16]

The Committee, and ultimately the Congress, moved quickly to enact restrictions on the use of pretexting to obtain confidential financial data. But the Committee's jurisdiction precluded it from addressing the pretexting of phone records, or other personal data.

**Operation Pretext Detect**

In April 1999, prior to the effective date of the GLB Act, the FTC filed suit against Touch Tone Information Systems, Inc., alleging that its use of pretexting constituted a deceptive and unfair practice in violation of the Federal Trade Commission Act. Touch Tone settled the charges in 2000.[17]

In January 2001, the FTC staff announced it was launching "Operation Detect Pretext," an effort to protect consumers from firms that obtain their customer information under false pretenses. As part of the operation, FTC staff conducted a "surf" of more than 1,000 Web sites and a review of more than 500 advertisements in the print media for firms that offered to conduct financial searches. The FTC staff then sent notices to approximately 200 firms by e-mail or

---

[16] Testimony of Evan Hendricks, Editor/Publisher, *Privacy Times*, House Committee on Banking and Financial Services, July 28, 1998 http://financialservices.house.gov/banking/72898hen.htm

[17] "Information Brokers Settle FTC Charges – 'Pretexting' To Obtain Consumers' Private Financial Data Barred, FTC Press Release, June 27, 2000; http://www.ftc.gov/opa/2000/06/touchtone.htm

facsimile advising them that their practices must comply not only with GLB's pretexting restrictions, but with other applicable federal laws, including the Fair Credit Reporting Act. The notice advised the firms that the FTC would continue to monitor Web sites and print media advertisements offering financial searches, and asked them to take steps to ensure that they complied with GLB and all other applicable federal laws.

In April 2001, the FTC filed separate suits against three more data brokers, charging that their use of false pretenses to steal consumers' private financial information and sell it violated the FTC Act and the Gramm-Leach-Bliley Act. The FTC complaints named Information Search, Inc., and David Kacala of Baltimore, Maryland; Victor Guzzetta doing business as Smart Data Systems of Staten Island, New York; and Paula Garrett doing business as Discreet Data Systems of Humble, Texas. The cases were filed under seal in U. S. District Courts for the District of Maryland; the Eastern District of New York; and the Southern District of Texas.

Several lessons can be drawn from this history. First, it makes clear that underhanded methods, such as pretexts and bribes, are the principle means by which unethical data brokers obtain, or facilitate the obtaining, of confidential consumer records. Second, virtually every public reference to unethical brokers and their underhanded methods, whether it be Congressional hearings, enforcement actions by State AGs or the FTC, or print or television news coverage, made clear that these methods were highly objectionable, invasive of commonly accepted notions of privacy, and harmful to consumer victims. Third, that the public, as expressed through Congress and enforcement agencies, wanted the practices stopped. Fourth, that data brokers continued to make money and were unlikely to cease on their own as long as they stayed in the shadows, far away from spotlight. Fifth, that "sunshine" was proving to be the "best disinfectant" for curbing specific data brokers.

**Case Studies Involving The Use of Pretexts or Bribes To Obtain of Phone Records**

In recent years, several cases have surfaced in which data brokers such as the defendant in this case either obtained or facilitated obtaining the phone calling records of an individual without his or her knowledge or consent.

A few themes emerge from each of these cases. First, the data broker that is obtaining the victim's phone records by way of underhanded means such as pretexts or bribes is doing so because the broker has a paying client that is either seeking to take serious, adverse action against the victim, or investigating whether or not to do so. In some cases the motivation is purely economic. In other cases, it concerns political or corporate power. Still in others, it involves revenge and direct threats to health and safety – and even to life itself.

Second, the public reaction to such underhanded tactics is highly negative, explicitly reflecting that reasonable Americans view such tactics as unfair, highly intrusive and unconscionable.

Third, the victims of such underhanded tactics consistently express feelings of being violated.

Fourth, when educated consumers attempt to apply extra security measures to protect their cell phone records, like placing a required password, data brokers were still able to compromise the records.

**Christopher Byron**

Christopher Byron, a journalist with the *New York Post*, testified before Congress regarding what it was like to be the victim of having his phone records obtained without his knowledge or consent. Byron was working on a major story on what he described as shady characters who had partnered with former FBI Asst. Director Buck Revell in connection with a "facial-recognition" technology company called Imagis Technology.

After interviewing Revell, operatives presumably connected to Imagis tried on 48 occasions to obtain Byron's phone records for July 2002 – the month that Bryon had interviewed Revell and other sources for his critical story of Imagis. The operatives finally obtained them on October 15, 2002, Byron testified, citing AT&T computer logs. Byron said that Imagis, a Vancouver, B.C. company, obtained his phone records in order to prepare its libel lawsuit against Byron, which it subsequently filed in Canadian court.

In his prepared statement, Byron described some of the negative impacts of being the victim of the underhanded seizure of his phone records by those unauthorized persons who were out to do him harm.

> I make these suggestions solely because of the first-hand experience both I and my family have had as victims of this nefarious practice. Though I alone was targeted by these so-called pretexters (I prefer the more accurate and less sanitized phrase, "criminal impersonators") the activities they set in motion quickly enveloped my wife and our three children as well as myself. And during the four years that have followed, our lives have been convulsed in ways that set our nerves on edge even now, whenever the phone rings unexpectedly or at an odd hour in my home office.
>
> To discover that someone has spent weeks trying to obtain access to you and your family's most personal and private records, and finally succeeded is like learning that a Peeping Tom has been spending weeks on end hovering at night outside your bedroom window, watching and videotaping everything that goes on inside.
>
> And it doesn't end there. When a pretexter goes unpunished, his victims can easily enough start to worry about things that never before concerned them – things they can ultimately do nothing about except worry even more, until all of

life becomes a parade of imagined catastrophes. Is someone reading my mail? Is there a tap on my phone line? A bug in my bedroom?

**Hewlett-Packard**

The most highly publicized case of underhanded obtaining and use of cell phone records surfaced this year in the case of Hewlett-Packard's executives investigating news leaks by members of its Board of Directors. In seeking to uncover the source of leaks, HP executives agreed that an investigative firm it retained could use pretexting and other underhanded methods to obtain the phone records and other personal data on Board Members Tom Perkins and George "Jay" Keyworth and several journalists.

Of particular relevance here was that the story broke in part due to Perkins' outrage over the Board meeting minutes in which HP General Counsel Ann Baskins described Perkins as having "concurred" with the nature of the board's investigation into leaks to reporters. Perkins wrote Baskins and Chief Executive Mark Hurd that he did not know before the May 18 meeting the investigation involved checking people's phone call records.[18]

"I had no idea that personal communications were involved, and had I known that this was the case I would have brought the matter . . . to the board," Perkins wrote in mid-July.[19]

Ten days later, when no one had responded to his request that the board minutes be revised, Perkins told the board he had hired a Washington lawyer. He asked the board to take up a full investigation of what he believed to be secret surveillance with illegal phone-record snooping by consultants hired by HP to help find the boardroom leaker. Two months later, the disagreement exploded in public. HP disclosed on Sept. 6 to the Securities and Exchange Commission that Perkins resigned at the board meeting where results were presented of the investigation into boardroom leaks. In its statement to the SEC, HP also said that Perkins had

---

[18] Therese Poletti and Dean Takahashi, "Inside the HP Saga: How Not To Fix a Leak, Or, How an Effort to Fix a Problem Created a Bigger One," *San Jose Mercury News*, Oct. 14, 2006; http://www.mercurynews.com/mld/mercurynews/news/15767017.htm

[19] *Id.*

asked the company about the methods used in the investigation, including "pretexting" or impersonating people to get their phone records without their knowledge.[20]

**L.A. Police Officers**

In 1998, the Los Angeles Police Department (LAPD) had a serious security problem. Suspected mobsters obtained home phone numbers and addresses of detectives. In an apparent attempt at intimidation, one mobster showed up at a police officer's home while he was at work, gave his name to the officer's wife and walked away. The LAPD eventually determined that the officers' personal data came from a Denver company, Touch Tone Information Inc., which used a technique known as "pretexting." Touch Tone workers would call phone companies and records holders pretending to be regulators, customers or employees and get them to divulge account information.[21]

According to the Associated Press, the case "stirred outrage."

The Federal Trade Commission forced Touch Tone out of business, and its owner, James Rapp, spent a few months in jail. Robert Pitofsky, chairman of the FTC at the time, said, "This case should send a strong message to information brokers that the FTC will pursue firms that use false pretenses to profit at the expense of consumers' privacy."[22]

---

[20] *Id*

[21] Peter Svensson (Associated Press),"Phone-Record Sellers Facing Renewed Scrutiny: Web Sites Say They Aren't Breaking Law," *San Diego Union-Tribune*, January 19, 2006

[22] *Id.*

**Murder Case**

Luis Alberto Gomez-Rodriguez, who is charged with the double-murder of Maria Antonia Rivero and Juan Sarol-Cepero, allegedly was able to locate the couple by obtaining Sarol-Cepero's cell phone records and other personal data.[23]

**Adam Yuzuk**

Adam Yuzuk, a New York businessman, discovered that his Cingular cell phone calling records had been accessed multiple times, allegedly by Steve Kahn and Michelle Gambino, who was implicated in the Amy Boyer murder case in New Hampshire. By filing suit against Cipriani Accessories and others allegedly involved, Yuzuk was able to uncover a retainer agreement dated May 9, 2005 between Gambino Information Services and The Max Leather Group signed by Michelle Gambino and Steve Kahn. It states "Cellular Phone records shall also be conducted as part of the request of the CLIENT, The COMPANY'S fee for this investigation will be $300.00 (Three Hundred Dollars)." The data brokers obtained Yuzuk's cell phone calling records from May 2005 to September 2005. "This means that someone broke into my Cingular account two additional times after my account was password protected and I was given what I believed was the highest level of security," Yuzuk testified before Congress. Subsequently, Cingular filed suit against Cipriani Accessories/Steve Kahn and Gambino Information Services in the Northern U.S. District Court of Georgia, requesting damages and "replevin of the documents." After the Amy Boyer murder case in New Hampshire, how is Gambino still in business and openly selling telephone information?[24]

---

[23] Stephen Byrd, "The Hunt Begins: Witnesses Tell of Suspect's Methodical Search for Muscatine Couple," *The Muscatine Journal*;
http://www.muscatinejournal.com/articles/2006/02/11/news/doc43ed6d7e5ba1f[illegible]

[24] Testimony of Mr. Adam Yuzuk, "Internet Data Brokers and Pretexting: Who has Access to Your Private Records?" House Energy and Commerce Subcommittee on Oversight and Investigations Hearing, June 21, 2006; http://energycommerce.house.gov/108/Hearings/06212006hearing1926/Yuzuk[illegible].pdf

**Wireless Phone Firms: Additional Costs & Inconvenience To Businesses & Consumers**

As illustrated by the testimony below, the advent of unethical data brokers who obtain, or facilitate the obtaining of, confidential consumer records by using underhanded methods, such as pretexts and bribes, has forced wireless companies to incur extra costs to protect the information. What should be noted is that phone company officials state that because of the dynamics of the ever-evolving world of data brokers, they will continue to incur additional costs indefinitely. Moreover, the new safeguards have made it less convenient for consumers to get access to their own records for legitimate purposes.

- Cingular Wireless changed its internal access procedures so call detail records would no longer be provided over the phone. Cingular also filed lawsuits against "locatecell.com" and "efindouthetruth.com," obtaining court injunctions against the operators of both Web sites. Subsequently, it brought four more lawsuits against more than 30 different corporate and individual defendants.[25]
- Cingular's representative told Congress: "We know that this is a fight that will never be over – the data burglars will always be out there, continually evolving their methods, and we will be continually working to counter their efforts.[26]
- Verizon Wireless filed suit and won preliminary injunctions against Data Find Solutions and First Source Information Specialists, the current and former owners of the Web sites locatecell.com, celltolls.com, peoplesearchamerica.com and data find.org. Moreover, Verizon Wireless filed suit and ultimately obtained a permanent injunction against Source Resources, Inc., which advertised on the Web that it could obtain cell phone records. Verizon Wireless obtained a temporary restraining order

[25] Statement of Thomas M. Meiss, Associate General Counsel, Cingular Wireless, House Energy & Commerce Subcommittee on Oversight & Investigations, September 29, 2006.
[26] *Id.*

against Global Information Group (GIG), which allegedly made thousands of attempts to steal confidential information without proper authorization.[27]

- Gregory Schaffer, Alltel's Chief Security Officer, testified that adequate protection for cell phone records was an ongoing process that would entail costs indefinitely. "Understanding the current methods employed by all of these types of actors to obtain unauthorized access to records is instructive, but at Alltel we also worry about anticipating future techniques. We know that any static approach to preventing unauthorized access ... will quickly become obsolete. Instead our practices must have the flexibility to evolve to meet constantly changing technical and social engineering threats. Part of my job is devoted to strategically anticipating those future threats and designing methods and practices to defeat them.[28]

**'Privacy' Is Defined By 'Fair Information Practices'**

While recognizing that "privacy" is quite a broad topic, the U.S. Supreme Court declared unanimously in 1989, "To begin with, both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person."[29]

It is well established in the community of privacy experts – both in the United States and internationally – that in the "Information Age," privacy is defined by, and measured according to, the principles of "Fair Information Practices" (FIPs).

A discussion of FIPs is relevant here, because FIPs are based on the premise that unreasonable, invasive information practices are harmful to consumers. FIPs are designed to prevent those harms by setting standards relating to organizational duties and individual rights.

---

[27] Statement of Michael Holden, Litigation Counsel, Verizon Wireless, House Energy & Commerce Subcommittee on Oversight & Investigations, September 29, 2006.
http://energycommerce.house.gov/108/Hearings/09292006hearing1947/Holden.pdf

[28] Statement of Greg Schaffer, Chief Security Officer, Alltel Wireless, House Energy & Commerce Subcommittee on Oversight & Investigations, September 29, 2006.

[29] U.S. Dept. Of Justice v. Reporters Committee, 489 U.S. 749 (1989)

As the U.S. Privacy Protection Study Commission (PPSC) said, it was vital that society adhere to Fair Information Practices in order to avoid harms to consumers. "[Our] findings reflect the fact that in American society today, records mediate relationships between individuals and organizations and thus affect an individual more easily, more broadly and often more unfairly than was possible in the past."[30]

A discussion of FIPs is also relevant because under any of the various articulations of these principles, Defendant's practices were blatantly unreasonable.

As explained in Chapter 10 of my book,[31] these principles are at the core of information privacy laws, both in the United States and abroad, including the FCRA and the U.S. Privacy Act.[32] They seek to ensure that individuals maintain a reasonable level of control over their personal information by ensuring accuracy, fairness, collection and use limitation, purpose specification, security, and enforcement. These principles form the basis for an international consensus[33] as to how personal data should be protected by law and by organizational practice. These principles reflect the view that for privacy to be adequately protected, organizations must observe an array of practices to ensure that personal information is treated fairly and accurately. They also reflect the view that privacy protection requires that organizations handling personal data assume responsibilities and that individuals are granted certain rights.

The principles have evolved somewhat, but have remained consistent at the core. The principles were first articulated in 1973 by the U.S. Department of Health, Education and Welfare Secretary's Advisory Committee on Automated Personal Data Systems. The report, entitled *Records, Computers and The Rights Of Citizens*, set forth the first five principles of Fair Information Practice:

---

[30] Personal Privacy In An Information Society: The Report of The Privacy Protection Study Commission (July 1977, Washington, D.C.).

[31] Credit Scores and Credit Reports: How The System Really Works, What You Can Do, [2nd Edition] (Privacy Times, 2005).

[32] (For example, the U.S. Court of Appeals for the First Circuit noted that "the Privacy Act . . . was based in part on the FCRA." (Sunday Dixon Orekoya v. James Mooney, U.S. Secret Service: CA-1st – No. 02-1306; May 15, 2003).

[33] "Principles of Fair Information Practices, Organization of Economic Cooperation and Development (OECD), 1980.

- There must be no personal-data record-keeping systems whose very existence is secret; (Transparency)
- There must be a way for an individual to find out what information about him is in a record and how it is used; (Notice)
- There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent; (Secondary use)
- There must be a way for an individual to correct or amend a record or identifiable information about him;
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of data.

In 1977, the U.S. Privacy Protection Study Commission (PPSC), a bipartisan panel created by the U.S. Privacy Act of 1974, endorsed these principles in recommending legislation to cover private sector records. The PPSC distilled FIPs into three general principles for guiding policy and for evaluating organizational information practices. They were: (1) minimize intrusiveness; (2) open up record-keeping operations in ways that will minimize the extent to which recorded information about an individual is itself a source of unfairness in any decision about him made on the basis of it (maximize fairness); and (3) create legitimate enforceable expectations of confidentiality.[34]

In the first paragraph of its introduction, the PPSC said it was vital that society adhere to Fair Information Practices in order to avoid harms to consumers.[35]

[34] PPSC Report, *op. cit.*
[35] *Id.*

In 1980, the Organization of Economic Cooperation and Development, based in Paris, adopted the following eight principles of fair information practices, still referred to by some experts as the "Gold Standard" of privacy.

- Collection Limitation
- Data Quality
- Purpose Specification
- Use Limitation
- Security Safeguards
- Openness
- Participation
- Accountability

These principles were endorsed by the governments of the United States, Japan and most Western European countries. These principles effectively have been recognized by the United Nations in its work on privacy.

These principles are at the core of many U.S. information-privacy laws, and also are at the core of the National Data Protection Laws of European countries, as well as Canada, New Zealand and Australia, and the European Union's Directive On Data Protection.

In the mid-1990s, when the Federal Trade Commission took the lead for establishing the U.S. Government's privacy policy on electronic commerce, it distilled the FIPs into five principles:

- Notice
- Choice/Consent
- Access
- Security
- Enforcement

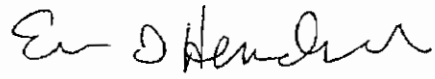
Applying the OECD guidelines, we can see that Defendant's underhanded tactics contravened principles of Collection Limitation, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness and Participation. If Defendant's legal theory is upheld by the Court, then the final principle – Accountability – would not apply.

**Executed This The 19th Day of November 2006, in Bethesda, Maryland**

**Evan D. Hendricks**
PO Box 302
Cabin John, MD 20818
(301) 229 7002

Applying the OECD guidelines, we can see that Defendant's underhanded tactics contravened principles of Collection Limitation, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness and Participation. If Defendant's legal theory is upheld by the Court, then the final principle – Accountability – would not apply.

**Executed This The 19th Day of November 2006, in Bethesda, Maryland**



**Evan D. Hendricks**
PO Box 302
Cabin John, MD 20818
(301) 229 7002

**BACKGROUND & QUALIFICATIONS (Curriculum Vitae Attached)**

My expertise in credit reporting stems from several of my professional activities, including:

(1) Editor/Publisher of a specialty news reporting service that covers credit reporting, Fair Information practices and related matters.

(2) Author of the book Your Right To Privacy: A Basic Guide To Legal Rights In An Information Society (2nd Edition, Southern Illinois University Press, 1990), which was possibly the first privacy book published with a chapter devoted to private investigators and how they were capable of obtaining most personal records, regardless of privacy laws, by using insider contacts and other surreptitious means. More recently, I am author of the book, Credit Scores and Credit Reports: How The System Really Works, What You Can Do, 2nd Edition, (Privacy Times 2005), which has a chapter on impermissible access.

(3) An expert witness qualified by Federal and State courts in litigation involving the collection, disclosure, use, maintenance and/or safeguarding of confidential consumer information. Many of theses cases were brought under the Fair Credit Reporting Act (FCRA), and some involved identity theft.

(4) An expert on data brokers who was one of the first privacy experts to identify brokers as having a significant impact on Americans' right to privacy. I testified at two of the earliest and most significant hearings held by Congress on the issue of data brokers and the threat they posed to privacy. The first was held in February 1992 by the Senate Finance Subcommittee on Social Security.[36] The second hearing was held in July 1998 by the House Banking Committee and was instrumental in enactment of the provisions to the Gramm-Leach-Bliley Act (GLB) that banned the use of pretexting, and separate

36 "Protecting the Privacy of Social Security Numbers and Records," Senate Finance Subcommittee on Social Security and Family Policy, February 28, 1992.

provisions requiring financial institutions to adopt safeguards to prevent the wrongful disclose or misuse of customer financial information.[37]

(5) An expert consultant to government agencies, including the Social Security Administration since 1998, and private corporations.

Since 1981, I have been Editor/Publisher of *Privacy Times*, a biweekly, Washington-based newsletter that reports on privacy and information law, including the Fair Credit Reporting Act (FCRA). The newsletter ranges from 8-12 pages, 23 issues per year. Thus, I have researched, written, edited and published many articles on Congressional and State legislative actions, judicial opinions, industry trends and actions, executive branch policies and consumer news as they related to information-privacy issues, including data brokers.

I am co-author of the book, Your Right To Privacy: A Basic Guide To Legal Rights In An Information Society (2nd Edition, Southern Illinois University Press, 1990), which was possibly the first privacy book with a chapter devoted exclusively private investigators and their ability to obtain confidential records regardless of privacy laws. I am also author of the book, Credit Scores and Credit Reports: How The System Really Works, What You Can Do (2nd Edition, Privacy Times 2005). The book has 23 Chapters, 403 pages and 369 footnotes. As the title indicates, it describes how the credit scoring and credit reporting systems work and what consumers can do to obtain their reports, read and understand them, correct errors in them and enforce their rights.

Since the early 1990s, I have served as an expert witness in numerous FCRA cases and have been qualified by federal and state courts. As an expert witness, I have had the opportunity to read thousands of pages of deposition testimony by consumer reporting agency officials and by credit grantor personnel responsible for reporting data to CRAs. This is significant because CRAs and credit grantors do not openly discuss or publish information on their procedures and practices for handling personal data. In fact, CRAs typically consider such procedures and practices to be proprietary and/or trade secrets.

[37] Testimony of Evan Hendricks, Editor/Publisher, *Privacy Times*, Committee on Banking & Financial Services, July 28, 1998 http://banking.senate.gov/98_07hrg/072898/hend.htm

I have testified before Congress – always by invitation – on numerous occasions, including once in 2006, three times in 2005, and four times in 2004. (see attached CV).

On December 3, 2002, I testified before the California State Senate Insurance Committee. On January 29, 2003, I testified before the California State Assembly Insurance Committee. Both Committees were considering financial privacy legislation (SB 1), which ultimately was enacted by the legislature and signed into law in September 2003.

I regularly present at Continuing Legal Education or professional seminars related to the FCRA, including Glasser LegalWorks (Sept. 2004), Privacy and American Business (Feb. 2004), and the National Credit Reporting Assoc. (Nov. 2004). In 2005, I presented at separate FCRA-related seminars sponsored by the Practicing Law Institute and Texas Bar Association, and was invited back to present at Glasser LegalWorks May 2005 FCRA seminar.

Two of the three major CRAs have acknowledged that I am an expert on credit reporting as it relates to "Fair Information Practices." First developed in the United States in the late 1960s, Fair Information Practices (FIPs) standards are at the core of the FCRA and most other U.S. and European privacy and data protection laws, and serve as an internationally accepted standard for gauging privacy policy and practices.

In 1990, Equifax published "The Equifax Report on Consumers In the Information Age," a nationwide opinion survey and analysis by Louis Harris and Associates and Prof. Alan F. Westin. The report listed me as a privacy expert to whom the authors expressed appreciation for my advice on survey coverage.

In April 2002, I accepted Experian's invitation to serve on the Experian Consumer Advisory Council of Experian (formerly TRW), a national CRA and vendor of other information services. Before being disbanded in 2004, the Council met twice a year to offer non-binding advice and to discuss a host of credit reporting, marketing and other privacy-related topics.

In 2004, I passed an industry examination, thereby earning "FCRA Certification" from the National Credit Reporting Association.

Since August 1998, I have served under contract as a member of the Social Security Administration's Panel Of Privacy Experts advising the agency on a host of issues.

(Please consult the attached CV for additional information.)

**TESTIMONY AND EXPERT REPORTS**

Within recent years, I have testified at trial, or been deposed as an expert, in the following cases:

Andrews v. Trans Union Corp. et al., Case No. 96-7369, (USDC-C.D. Calif.), concerning theft-of-identity and consumer report inaccuracies. Expert report, deposition, trial testimony. Judge Lourdes Baird qualified me to testify about identity theft and its impact on the consumer. The U.S. Court of Appeals for the Ninth Circuit ruled that jury would have been assisted by my testimony, regarding the prevalence of identity theft in evaluating the reasonableness of CRA procedures. (see 225 F.3d 1063 (2000)).

Suzanne Sloane vs. Equifax Information Services, LLC, et al., U.S. District Court for the Eastern District of Virginia (Alexandria Div.), Case No. CIV 1:05 cv 1272. Expert reports. Deposition. Trial Testimony Judge Leonie M. Brinkema presiding.

Matthew Kirkpatrick. v. Equifax Credit Information Services, et al.: U.S. District Court for the District of Oregon; No. CV 02-1197-MO. FCRA, identity theft. Expert report. Deposition. Trial Testimony. Judge Michael W. Mosman presiding.

Eddie Silva, et al. vs Haynes Furniture Co., Inc.: U.S. District Court for the Eastern District of Virginia: No. 4:04CV82. FCRA. Trial Testimony. Judge Walter D. Kelley, Jr. presiding.

Joi Helmes v. Wachovia Bank N.A.: U.S. Bankruptcy Court for the Eastern District of Virginia (Alexandria), Case No: 01-81277-RGM, Chapter 7. Post-bankruptcy credit reporting. Expert report. Deposition. Trial Testimony. Judge Robert G. Mayer presiding.

Denis W. Stasulis v. Suntrust: U.S. Bankruptcy Court for the Eastern District of Virginia (Alexandria), Case No: 04-12542-RGM, Chapter 7. Post-bankruptcy credit reporting. Expert report. Deposition. Trial Testimony. Judge Robert G. Mayer presiding.

Sandra Cortez vs. Trans Union, LLC., U.S. District Court for the Eastern District of Pennsylvania: No. 2:05 –cv—05684-JF. FCRA. Expert Report. Daubert Hearing. Senior Judge John P. Fullum qualified me to testify at trial.

Dwaine Perry, et al. v. FleetBoston Financial Corp.: U.S. District Court for the Eastern District of Pennsylvania: No. 04-507. FCRA. Expert Report. Fairness hearing testimony. Judge Berle M. Schiller presiding.

Tammy Cochran v. C&M Motors, LLC, dba I-10 Toyota, et al: U.S. District Court for the Central District of California, No. CV-03-3568FMC. FCRA. Expert Report. Trial Testimony. Judge Florence-Marie Cooper presiding.

Myra Coleman v. Trans Union LLC, CA4: 98-CV-169B-B (USDC-Mississippi) FCRA. Expert report, deposition, trial testimony. Judge Neal B. Biggers presiding.

Arthur Spengler v. Sears Roebuck & Co., Case No. C-03-0557. (Circuit Court, Wicomico County, Maryland). Tort, Interference with Business Relationships. Trial Testimony. Judge D. Davis qualified me as expert on credit scoring, credit reporting and FCRA-related issues.

Judy C. Thomas v. Trans Union LLC, U.S. District Court for the District of Oregon; Case No. 00-1150-JE. FCRA. Expert report, deposition, trial testimony. Magistrate Judge John Jelderks presiding.

Scott E. Campbell v. G.E. Capital Auto Lease, Circuit Court For St. Mary's County, Maryland, Case No. 99-522. FCRA, invasion of privacy. Expert report, deposition. Judge Karen Abrams qualified me to testify, but the case settled one week before trial.

Franklin F. Grizzard, Jr. v. Trans Union, L.L.C., & Equifax Information Services L.L.C., et al.: U.S. District Court for the District of Virginia (Richmond Div.); Nos. 04-CV-625 & 04-CV-626, respectively. Expert report. Affidavit. Deposition. On the eve of trial, Judge Richard Williams rejected Defendant's motion to disqualify me. The case settled shortly thereafter.

Franklin E. Clark, et al. v. Experian, et al.: U.S. District Court for the District of South Carolina, Case Nos. 8:00-1217-22, 8:00-1218-22, 8:00-1219-22. Affidavit, Supplemental Affidavit (both affidavits were admitted into evidence without objection). Judge Cameron McGowan Currie presiding.

In Re: Farmers Insurance Co., Inc., FCRA Litigation, U.S. District Court for the Western District of Oklahoma, Case No. CIV 03-158-F. FCRA. Expert report, deposition.

Steven E. Beck v. Equifax Information Services, et al.: U.S. District Court for the Eastern District of Virginia: No. 1-05cv347. FCRA. Expert report, deposition.

Larry Alabran v. Capital One Services, Inc.,: U.S. District Court for the Eastern District of Virginia (Richmond Division); Case No. 3:04-CV-935. Expert report, deposition.

Gail Cope v. MBNA American Bank NA: U.S. District Court for the District of Oregon; No. 04-CV-493-JE. Expert report, deposition.

Robert Gordon Peoples v. Experian Services Corp., et al.: U.S. District Court for the Central District of California: No. CV-04-1378 CAS (Ex). Expert report. Deposition.

Lottie Robertson v. Experian Information Services, Inc. & Capital One Bank: U.S. District Court for the Eastern District of Michigan (Southern Div.) No. 04-72308. Expert report. Deposition.

Barbara A. Harris v. Experian Information Solutions, Inc., and Equifax Credit Information Services, Inc: U.S. District Court for the District of Oregon, Civil No. 01-1728-JE. FCRA. Expert reports. Deposition.

Bruce Danielson v. Experian Information Solutions: U.S. District Court for the Northern District of Texas, Case No: 3-04CV-1722N. FCRA. Expert report. Deposition.

Stacy Lawton Guin, et al. v. Brazos Higher Education Service Corporation, Inc.: USDC-Minnesota – No. CV 05-668 RHK/JSM. Negligence. Security Breach. Affidavit. Deposition.

Anthony Chin v. State Dept. Federal Credit Union: Circ. Ct. Prince George's County (Maryland); Civ. Act. No. CAL04-12778; Tort. Deposition.

James M. McKeown v. Sears Roebuck & Co., et al: U.S. District Court for the Western District of Wisconsin, Civil No. Case No. 03-CV-0528 C. Expert Report, deposition.

Paulette Field v. Trans Union LLC, et al., Case No. 01 C 6390 (USDC-N.D. Illinois - Eastern Div. FCRA. Expert report. Deposition.

Earle E. Ausherman, et al. v. Bank of America Corporation et al.: U.S. District Court for the District of Maryland, Civil Action No. MJG-01-438. FCRA. Expert report. Deposition

Jesse Kleo v. Elmhurst Dodge, U.S. District Court for the Northern District of Illinois (Eastern Division) Civil Action No. 01 C 0433. FCRA. Expert report, deposition

David & Ruthie Keefner v. Webb Ford, Inc. & Deon L. Willis.: U.S. District Court for the Northern District of Illinois (Eastern Division), Civil Action No. 02C-4643. FCRA. Expert report. Deposition.

Anthony & Alethea Preston v. MGIC, U.S. District Court for the Middle District of Florida (Ocala), Case No. 5:03-cv-111-Oc-10GRJ. FCRA. Expert report, deposition.

Bruce Butcher and Pam Butcher v. Chase Manhattan Bank, U.S.A., Inc., U.S. District Court for the District of South Carolina, Case No. 8:03-3184-26. FCRA. Expert report, deposition.

Catherine Smith, et al. v. Progressive Corporation, et al.: U.S. District Court for the Middle District of Florida (Gainesville), Case No.1:00-CV-210-MMP. Expert Report, Declaration of Value.

**FEE**

My fee is $250 per hour for preparation and for consulting; $250 per hour, or a minimum of $1,000 per day, for deposition or trial testimony, plus reasonable travel time, plus travel costs and expenses.

# *Evan Hendricks*

## *CURRICULUM VITAE*

**Professional Activities**

1981- Present **Editor/Publisher** of ***Privacy Times***

Since 1981, I have been Editor/Publisher of *Privacy Times*, a biweekly, Washington-based newsletter that reports on privacy and information law, including the Fair Credit Reporting Act (FCRA). The newsletter ranges from 8-12 pages, 23 issues per year. Thus, I have researched, written, edited and published many articles on Congressional and State legislative actions, judicial opinions, industry trends and actions, executive branch policies and consumer news as they related to the FCRA.

**1992 – Present Expert Witness**

Qualified by the federal courts in FCRA and identity theft cases. (Complete list attached). I have read extensive deposition testimony by credit bureau and credit grantor personnel. This is significant because CRAs and credit grantors do not openly discuss or publish information on their procedures and practices for handling personal data, and the best (and possibly only) sources for finding candid descriptions of CRAs' and credit grantors' procedures and practices in relation to credit reporting data are the depositions of CRA and credit grantor employees in FCRA litigation.

**1998 – Present Privacy Expert Consultant, U.S. Social Security Administration**

Regularly review policies and practices in relation to the collection, use and disclosure of personal data and Social Security numbers and provide feedback and recommendations.

**2002 – 2004 Member, Experian Consumer Advisory Council**

Along with other Council members, I provide an outsider's view on credit reporting, marketing and other privacy issues.

---

**Evan Hendricks P.O. Box 302 Cabin John, MD 20818**
**(301) 229 7002 (301) 229 8011 [fax]** evan@privacytimes.com

---

**July – October 2002 Consultant to U.S. Postal Service**

Working with the USPS's Chief Privacy Officer, I assisted in reviewing and editing the re-write of the USPS's Privacy Act notices, with an emphasis on "Plain English."

**Recent Testimony Before Congress & The FTC**

"Privacy in the Commercial World II," House Energy & Commerce Subcommittee On Commerce, Trade, and Consumer Protection, June 20, 2006[38]

"Financial Data Protection Act of 2005," House Financial Services Subcommittee on Financial Institutions and Consumer Credit, November 9, 2005[39]

"Credit Card Data Processing: How Secure Is It?" House Financial Services Subcommittee on Oversight and Investigations, July 21, 2005[40]

"Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information,"[41] Senate Banking Committee, March 15, 2005

"The Accuracy of Credit Report Information and the Fair Credit Reporting Act;" Senate Banking Committee, July 10, 2003[42]

"The Role of FCRA in the Credit Granting Process," House Financial Services Subcommittee on Financial Institutions & Consumer Credit, June 12, 2003[43]

"Database Security: Finding Out When Your Information Has Been Compromised," Senate Judiciary Subcommittee on Technology, Terrorism and Government Information, Nov. 4, 2003[44]

"Fighting Fraud: Improving Information Security," House Financial Services Subcommittee on Financial Institutions & Consumer Credit, and Oversight, April 3, 2003[45]

"Information Flows: The Costs and Benefits to Consumers and Businesses of The Collection and

---

[38] http://energycommerce.house.gov/108/hearings/06202006hearing1955/Hoofnagle1955.pdf

[39] http://financialservices.house.gov/hearing.asp?formmode=detail&hearing=

[40] http://financialservices.house.gov/hearing.asp?formmode=detail&hearing=

[41] http://banking.senate.gov/index.cfm?FuseAction=Hearings.Detail&HearingID=

[42] http://banking.senate.gov/03_07hrg/071003/index.htm

[43] http://financialservices.house.gov/hearing.asp?formmode=detail&hearing=

[44] http://govinfo.library.unt.edu/crb/crb03/pdf/

[45] http://financialservices.house.gov/hearing.asp?formmode=detail&hearing=

Use of Consumer Information," Federal Trade Commission, National Workshop, June 18, 2003

**Books**

Credit Scores and Credit Reports: How The System Really Works, What You Can Do [2nd Edition] (Privacy Times, 2005)

Your Right To Privacy: A Basic Guide To Legal Rights In An Information Society (2nd Edition, Southern Illinois University Press, 1990), (Includes a chapter on credit reporting)

Former Secrets: Government Records Made Public Through The Freedom of Information Act (Campaign For Political Rights, 1982)

**International Lectures**

24th International Conference of Data Protection & Privacy Commissioners (Cardiff, Wales – Presentation published in conference proceedings, 2002)
The 23rd International Conference of Data Protection Commissioners (Paris, La Sorbonne – Presentation published in conference proceedings, 2001)
The 22nd Annual Conference on Data Protection (Venice, Italy -- 2000)
The 16th Annual Conference on Data Protection (The Hague, The Netherlands -- 1994).

In the 1980s, served as an expert consultant to both the Privacy Commissioner of Canada and Privacy Commissioner of Australia.

**Presentations/Instruction At Recent CLE & Professional Seminars**

"11th Annual Consumer Financial Services Litigation," Practicing Law Institute, March 20-21, 2006 (New York City)
"Bankruptcy Roundtable," and, "Fair Credit Reporting Act Roundtable," National Consumer Law Center, October 27, 2005
"Advanced Consumer Litigation," Texas Bar CLE, Feb. 10-11, 2005
"Financial Privacy Litigation," (Impact of FACT Act), Practicing Law Institute, February 28- March 1, 2005 (New York City)
"The New FACT Act: Challenge & Opportunity," Privacy & American Business, Feb. 9-10, 2004
"Understanding the FACT Act And The Impact of Multi-Agency Rulewriting Process," Glasser LegalWorks, Sept. 28-29. 2004
"12th Annual National Conference," National Credit Reporting Association, Nov. 10-12, 2004

**Professional Societies**

Past President and Board Member, American Society of Access Professionals
www.accesspro.org

**Industry Certification**

FCRA Certification, National Credit Reporting Association ([illegible]).

**Media**

In addition to being a paid consultant and special guest on CNN's IMPACT news in 1996, I am quoted regularly by major and small newspapers (including The Washington Post, New York Times, Wall Street Journal, Chicago Tribune, Los Angeles Times, Newsweek and Money Magazine), regarding issues of privacy generally and the privacy implications of consumer reporting specifically. I have appeared on National Public Radio, PBS NewsHour with Jim Lehrer, ABC Nightline and World News Tonight, NBC Nightly News, CBS Evening News, CNN News Watch, CNBC, MSNBC, Fox News, various local affiliates, and the Oprah Winfrey Show and Geraldo, regarding these issues as well.

**Education**

Bachelor of Arts, Columbia College, Columbia University, New York, N.Y. (1979)